User Manual
NB1600 Router Family

11-Apr-2012

Wireline UMTS/LTE WLAN WIAP

Table of Content

1 Safety and Conformity 5

1.1 Safety Instructions 5
1.2 Declaration of Conformity 6
1.3 Waste Disposal 6
1.4 National Restrictions 6
1.4.1 France 6
1.4.2 Italy 6
1.4.3 Latvia 6
1.4.4 Luxemburg 6
1.4.5 Norway 7
1.4.6 Russian Federation 7
1.4.7 Turkey 7

2 Hardware Specifications 8

2.1 Operating Elements 8
2.2 Interfaces 9
2.3 Pin Assignments 10
2.3.1 Terminal Block 10
2.3.2 Ethernet 10

3 Installation 11

3.1 Environmental Conditions 11
3.2 Installation of the Router 11
3.2.1 Installation of the SIM Card 11
3.2.2 Installation of the GSM/UMTS Antenna 11
3.2.3 Installation of the WLAN Antennas 11
3.2.4 Installation of the Local Area Network 11
3.2.5 Installation of the Power Supply 11

4 Configuration via Web Manager (Recommended) 12

4.1 Initial Access to the Web Manager and Setting the Administrator Password 12
4.2 Home 13
4.3 Interfaces 14
4.3.1 Ethernet Port Assignments 14
4.3.2 WAN 14
4.3.3 Ethernet 18
4.3.4 Mobile (2G, 3G, 3G+, 4G) 20
4.3.5 WLAN 23
4.3.6 USB Port 26
4.3.7 Serial Port 28
4.3.8 Digital I/O 30
4.4 Routing 31
4.5 Firewall 32
4.5.1 Firewall Administration and Rules 32
4.5.2 NAPT 33
4.6 VPN 36
4.6.1 OpenVPN 36
4.6.2 IPsec 39
4.7 PPTP Server 41
4.8 Dial-in Server 42
4.8.1 Dial-in Server Administration 42
4.8.2 Dial-in Server Configuration 42
4.9 Services 43
4.9.1 DHCP Server 43
4.9.2 DNS Proxy Server 44

4.9.3 Dynamic DNS 45
4.9.4 E-mail Client 46
4.9.5 Event Manager 47
4.9.6 SMS 50
4.9.7 SSH /Telnet Server 51
4.9.8 SNMP Agent 51
4.9.9 UDP Message Receiver 54
4.9.10 Unstructured Supplementary Services Data (USSD) 54
4.9.11 Web Server 55
4.9.12 Redundancy 56
4.10 System 57
4.10.1 Settings 57
4.10.2 Time and Region 58
4.10.3 System Information 59
4.10.4 Restart 59
4.10.5 Authentication 60
4.10.6 User Accounts 60
4.10.7 Remote Authentication 61
4.10.8 File Configuration 62
4.10.9 Troubleshooting 64
4.10.10 Software Update 66
4.10.11 Licensing 68
4.10.12 Keys and Certificates 68
4.11 Logout 68

5 Configuration via Command Line Interface (Advanced) 69

5.1 CLI Overview 69
5.2 CLI Usage 70

6 Software Interfaces 74

6.1 Digital I/O Server 74
6.1.1 Monitor the digital inputs and outputs 74
6.1.2 Set digital outputs 74
6.1.3 Get status of digital inputs and output 74
6.2 HTTP Service Interface 75
6.2.1 Command Set 75
6.2.2 Responses 76
6.2.3 Examples 77

7 Troubleshooting 78

7.1 Error Messages 78
7.2 System Log and Log Files 78
7.3 Network Protocol Analyzer 78

8 Customer Service 79

8.1 Technical Support 79
8.2 Feedback 79

1 Safety and Conformity

Thank you for purchasing a NetBox Wireless Router from NetModule. This chapter gives you an introduction to the router and its features. The following chapters describe the installation procedure and provide helpful information for configuration.

1.1 Safety Instructions

NetBox Wireless Routers must be used in compliance with any and all applicable international and national laws and in particular with any special restrictions regulating the utilization of communication modules in prescribed applications and environments.

It is highly recommended to use only the original accessories to prevent possible injury to health and damage to appliances and to ensure that all the relevant provisions have been complied with. Unauthorized modifications or utilization of accessories that have not been approved may void the warranty.

The NetBox Wireless Routers must not be opened. Only the replacement of the SIM card is permitted.

All circuits connected to the interfaces of the NetBox Wireless Router must comply with the requirements of SELV (Safety Extra Low Voltage) circuits and are for indoor use only. Interconnections must not leave the building nor penetrate the body shell of a vehicle. Possible antenna circuits must be limited to overvoltage transient levels below 1500 Volts according to IEC 60950-1, TNV-1 circuit levels using safety approved components.

Use only with certified (CSA or equivalent) power supply, which must have a limited and SELV circuit output.

The NetBox Wireless Routers are designed for indoor use. Do not expose the communication module to extreme ambient conditions. Protect the communication module against dust, moisture and high temperature.

We remind the users of the duty to observe the restrictions concerning the utilization of radio devices at petrol stations, in chemical plants or in the course of blasting works in which explosives are used. Switch off the communication module when travelling by plane.

You must proceed with increased caution when using the communication module in close proximity of personal medical devices, such as cardiac pacemakers or hearing aids.

NetBox Wireless Routers may cause interference if it is in the proximity of TV sets, radio receivers and personal computers.

After configuration it is recommended that you should create a copy or backup of the configuration settings that are stored in the memory of the device. The configuration data can be downloaded using the Web Manager.

Do not work at the antenna installation during a lightning.

Always keep a distance bigger than 40cm from the antenna in order to reduce your exposure to electromagnetic fields below the legal limits. This distance applies to Lambda/4 and Lambda/2 antennas. Bigger distances apply for antennas with higher gain.

If not mounted on a DIN rail, the device must be installed so that one of the entirely closed case sides points towards ground. All connections of the 15-pin connector must be plugged. All threaded holes must be provided with screws or covered with metal.

Consult the manual for the installation. Adhere to the instructions documented in the user manual.

1.2 Declaration of Conformity

NetModule declares that under our own responsibility the products NetBox Wireless Routers comply with the relevant standards following the provisions of the Council Directive 1999/5/EC. The signed Declarations of Conformity can be found under the following addresses:

NB1600:
http://www.netmodule.com/store/products/nb1600_conformity_declaration_e.pdf

1.3 Waste Disposal

In accordance with the requirements of the council directive 2002/96/EC on waste electrical and electronic equipment (WEEE), ensure that at end-of-life you separate this product from other waste and scrap and deliver it to the WEEE collection system in your country for recycling.

1.4 National Restrictions

This product may be used in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

1.4.1 France

In case the product is used outdoors, the output power is restricted in some parts of the band. See the table below or check http://www.art-telecom.fr/ for more details.

Frequency Range (MHz)	Power (EIRP)	Restrictions
2400-2454	100 mW (20 dBm)	Only for indoor applications
2454-2483.5	10 mW (10 dBm)	If used outdoors
5470-5725		Relevant+ provisions for the implementation of DFS mechanism described in ETSI standard EN 301 893 V1.3.1 and subsequent versions

1.4.2 Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless operating within the boundaries of the owner's property, the use of this Wireless LAN product requires a 'general authorization'. Please check with http://www.comunicazioni.it/ for more details.

1.4.3 Latvia

The outdoor usage of the 2.4-GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details.

1.4.4 Luxemburg

General authorization required for network and service supply.

1.4.5 Norway

Frequency Range	Restrictions
2400.0-2483.5 MHz (WLAN b/g)	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund

1.4.6 Russian Federation

Frequency Range (MHz)	Power (EIRP)	Restrictions
2400.0-2483.5	100 mW (20 dBm)	Only for indoor applications
5150-5250	100 mW (20 dBm)	Permitted to use only for indoor applications, closed industrial and warehouse areas, and on board aircraft
5250-5350	100 mW (20 dBm)	1. Permitted to use for local networks of aircraft crew service communications on board aircraft in area of the airport and at all stages of flight. 2. Permitted to use for public wireless access local networks on board aircraft during a flight at the altitude not less than 3000 m
5650-5825	100 mW (20 dBm)	Permitted to use on board aircraft during a flight at the altitude not less than 3000 m

1.4.7 Turkey

Frequency Range	Restriction
5470-5725 MHz	Not implemented

2 Hardware Specifications

There are five different models of NB1600 available (from left to right):

- NB1600-Wireline
- NB1600-UMTS
- NB1600-LTE
- NB1600-WLAN
- NB1600-WIAP

2.1 Operating Elements

The following table describes the NB1600 status indicators:

Label	Colour	State	Function	Presence
Status	any green yellow	blinking solid solid	The device is busy due to startup, software or configuration update. The device is ready. The captions of the right bank apply. The device is ready. The captions of the left bank apply.	Always
PPPoE	green	on	PPPoE connection is up. PPPoE connection is down.	NB1600-Wireline NB1600-WLAN
Mobile	green	on blinking	Mobile connection is up. Mobile connection is down. The colour of the LED represents the signal quality: red=low, yellow=moderate, green=good	NB1600-UMTS NB1600-LTE NB1600-WIAP
VPN	green	on off	VPN connection is up VPN connection is down	Always
WLAN	green	on off	WLAN connection is up WLAN connection is down The colour of the LED represents the signal quality: red=low, yellow=moderate, green=good	NB1600-WLAN NB1600-WIAP
Out1	yellow	on off	Normally open output closed Normally open output open	Always
Out2	yellow	on off	Normally closed output is closed Normally closed output is open	Always
In1	yellow	on off	Input set Input not set	Always
In2	yellow	on off	Input set Input not set	Always

Table 1: The NB1600 status indicators

2.2 Interfaces

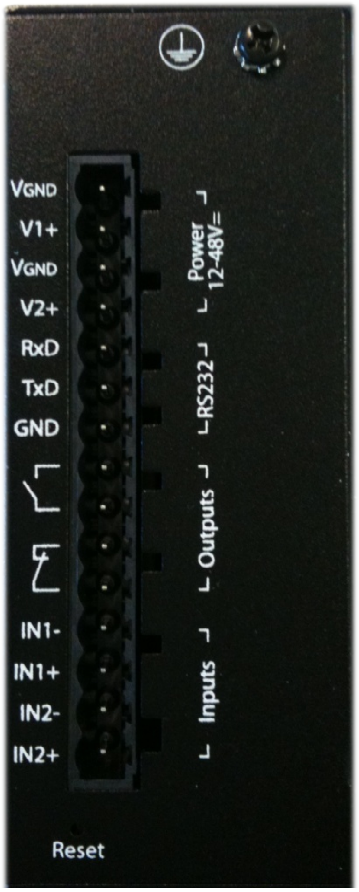
Label	Panel	Function	Presence
USB	Front	USB Host Port. To be used as USB device server or for software/configuration update.	Always
Ethernet 1	Front	First Ethernet Port. Can be used as LAN or WAN Port	Always
Ethernet 2	Front	First Ethernet Port. Can be used as LAN or WAN Port	Always
Mobile	Front	SMA female connector for GSM/UMTS antenna	NB1600-UMTS NB1600-WIAP
WLAN 1	Front	SMA female connector for first WLAN antenna (main)	NB1600-WLAN NB1600-WIAP
WLAN 2	Front	SMA female connector for second WLAN antenna (diversity)	NB1600-WLAN NB1600-WIAP
⏚	Top	Earth protection connector Earthing is optional. If used, connect a yellow-green marked cable with at least 6mm^2 cupper area. Avoid corrosion. Protect the screws against loosening. This connection is combined with the ground of the power supply (V_{GND}).	Always
Power	Top	Power supply 12-48V (Pin 1+2) Additional power supply (redundancy) 12-48V (Pin 3+4)	Always
RS-232	Top	Serial interface (Pins 5-7) which can be used for console administration, serial device server or other serial based communication applications.	Always
Outputs	Top	Digital outputs (Pins 4-11)	Always
Inputs	Top	Digital inputs (Pins 12-15)	Always
Reset	Top	Reset button, press at least 3 seconds for reboot and at least 5 second for factory reset. The initiation of the factory reset is confirmed with all LEDs lighting up for a moment. Then you can release the button.	Always

Table 2: The NB1600 interfaces

2.3 Pin Assignments

2.3.1 Terminal Block

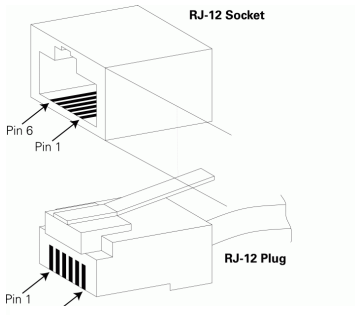
Pin:	Signal
1	V_{GND}
2	V1+ (12-48V=)
3	V_{GND}
4	V2+ (12-48V=)
5	RxD
6	TxD
7	GND
8	Out1: Dry contact relay Normally open
9	
10	Out2: Dry contact relay Normally closed
11	
12	In1-
13	In1+
14	In2-
15	In2+



00 terminal block

2.3.2 Ethernet

Pin:	Signal
1	TX+
2	TX-
3	RX+
4	-
5	-
6	RX-
7	-
8	-



re 2: RJ45

3 Installation

3.1 Environmental Conditions

The following precautions must be taken before installing NB1600:

- Avoid direct solar radiation.
- Protect the device from humidity, steam and aggressive fluids
- Guarantee sufficient circulation of air around the device.
- The device is for indoor use only
- Humidity: 0 to 95% (non-condensing)
- Altitude up to 4000m
- Overvoltage Category: II
- Pollution Degree: 2

3.2 Installation of the Router

NB1600 is designed for mounting it on a DIN rail or wall but it can also be put on a worktop. Please consider the safety instructions (chapter 1.1) and the environmental conditions (chapter 3.1).

3.2.1 Installation of the SIM Card

For installing a SIM card, you will have to remove the SIM cover first. The card holder is opened by sliding it slightly until it shifts up. You can now insert the SIM card, presses the holder and shift it back until it is locked. Ensure to have the contacts placed correctly, otherwise the holder will not lock. The cover has to be closed again.

3.2.2 Installation of the GSM/UMTS Antenna

NetBox Wireless Routers will only operate efficiently in the cellular network if there is a good signal. The provided stub antenna will be suitable for most applications. However, in some circumstances it might be necessary to use remote antennas together with an extended cable to reach a location which offers the best possible signal reception. NetModule can supply a range of suitable antennas.

Keep in mind that effects caused by Faraday cages such as large metal surfaces (elevators, machine housings, etc.); close meshed iron constructions and others can reduce signal reception significantly

Mount the antenna or connect the antenna cable to the antenna connector (Mobile).

3.2.3 Installation of the WLAN Antennas

Mount the WLAN antennas to the WLAN antenna connectors (WLAN). The number of attached antennas can be configured in the software. If only one antenna is used, it must be attached to WLAN 1 .

For better diversity and thus better throughput and coverage we recommend using both antennas.

3.2.4 Installation of the Local Area Network

Up to two 10/100 Mbps Ethernet devices can directly be connected to the NetBox.

3.2.5 Installation of the Power Supply

NetBox can be powered with the included power supply or another external source supplying between 12 and 48 Volts DC. NetBox is to be used with certified (CSA or equivalent) power supply, which must have a limited and SELV circuit output. The router is now ready for getting engaged.

4 Configuration via Web Manager (Recommended)

If you are new to NetBox we recommend the configuration using the Web Manager. For batch configurations you may upload configuration files, either using the Web Manager or triggered via SNMP, telnet or SSH. Advanced users can use the Command Line Interface (chapter 5).

The Web Manager supports the latest web browser (e.g. Microsoft Internet Explorer 9, Mozilla Firefox 8.0 and many others). Please ensure to have JavaScript turned on. By default the IP address of the Ethernet port 1 is set 192.168.1.1 and the DHCP server is turned on. Please apply the following steps for establishing your first Web Manager session:

Step	Description
1.	If not yet enabled, please enable the Dynamic Host Configuration Protocol (DHCP) so that your computer can lease an IP address from NetBox. This usually takes some time until your PC has received the corresponding parameters (IP address, subnet mask, default gateway, DNS server).
2.	Please connect the Ethernet 1 port of NetBox with the Ethernet port of your computer. You may take a look to your network control panel and check if your PC has correctly retrieved an IP address.
3.	Start a Web Browser on your PC and point it to the NetBox by entering the IP address in the address bar: http://192.168.1.1
4.	Please follow the instructions of the Web Manager in order to configure the device. Most of the menus are self-explanatory, further details are given below.

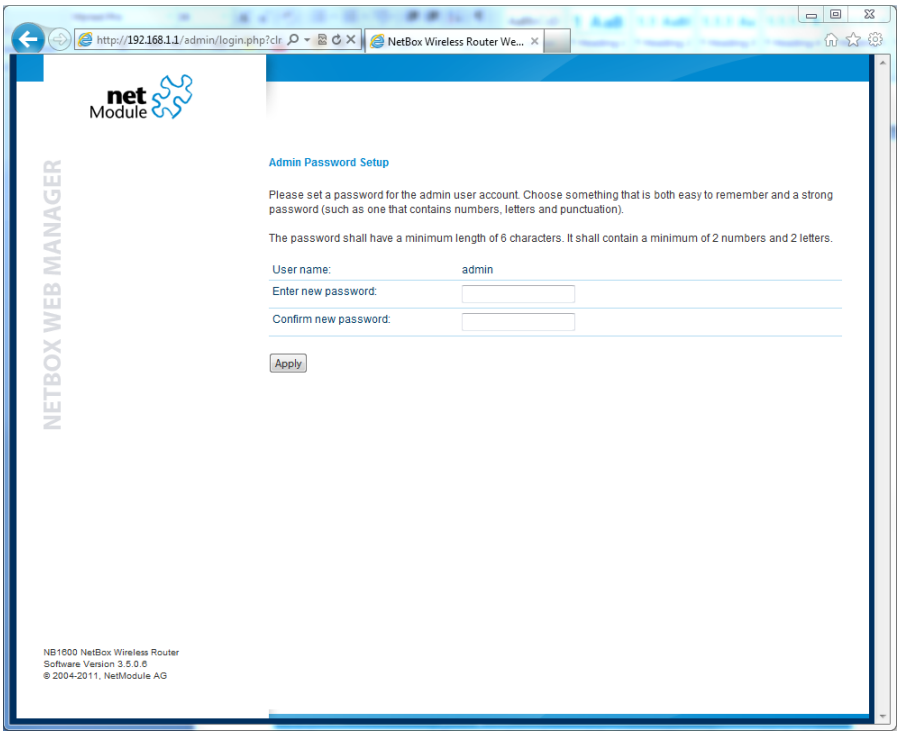
4.1 Initial Access to the Web Manager and Setting the Administrator Password

Please provide a password for the admin user account. Choose something that is both easy to remember and a strong password (such as one that contains numbers, letters and punctuation).

The password shall have a minimum length of 6 characters. It shall contain a minimum of 2 numbers and 2 letters.

Note: The admin password will be also applied for the root user which can be used to access the device over telnet/SSH and also to enter the boot loader.

With NetBox Software 3.5 you may also configure additional users which only have the permission to access the Dial-In/PPTP servers and the home/summary page.

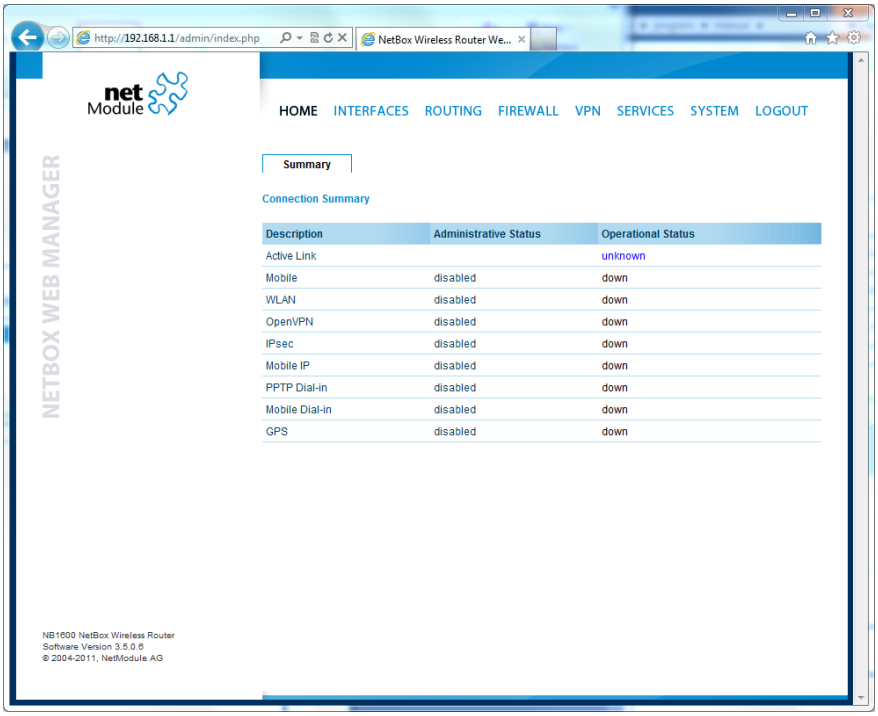

http://192.168.1.1/admin/login.php?clr
NetBox Wireless Router We...
net Module
NETBOX WEB MANAGER
Admin Password Setup
Please set a password for the admin user account. Choose something that is both easy to remember and a strong password (such as one that contains numbers, letters and punctuation).
The password shall have a minimum length of 6 characters. It shall contain a minimum of 2 numbers and 2 letters.
User name:
admin
Enter new password:
Confirm new password:
Apply
NB1600 NetBox Wireless Router
Software Version 3.5.0.6
© 2004-2011, NetModule AG

The minimum additional configuration steps for setting up a mobile connection conclude:

1. Defining the admin password
2. Entering the PIN code for the SIM card
3. Configuring the Access Point Name (APN)
4. Start the mobile connection

4.2 Home

This page provides a status overview of established connections and enabled features. It offers a summary and you can also get further details (such as the IP address, signal strength, data rates, etc).


http://192.168.1.1/admin/index.php
NetBox Wireless Router We...
net Module
NETBOX WEB MANAGER
HOME INTERFACES ROUTING FIREWALL VPN SERVICES SYSTEM LOGOUT
Summary
Connection Summary
Description | Administrative Status | Operational Status
Active Link | | unknown
Mobile | disabled | down
WLAN | disabled | down
OpenVPN | disabled | down
IPsec | disabled | down
Mobile IP | disabled | down
PPTP Dial-in | disabled | down
Mobile Dial-in | disabled | down
GPS | disabled | down
NB1600 NetBox Wireless Router
Software Version 3.5.0.6
© 2004-2011, NetModule AG

4.3 Interfaces

The interfaces section can be used to set up the physical interfaces and hardware features of NetBox.

4.3.1 Ethernet Port Assignments

The Netbox contains 2 external Ethernet ports named Ethernet 1 and Ethernet 2. Those ports have to be mapped to the internal logical names LAN1 and LAN2. This is done to have more flexibility at the external cable wiring. Afterwards the logic port names needs to be assigned to the functional area of the ports WAN or LAN.

4.3.2 WAN

4.3.2.1 Link Management

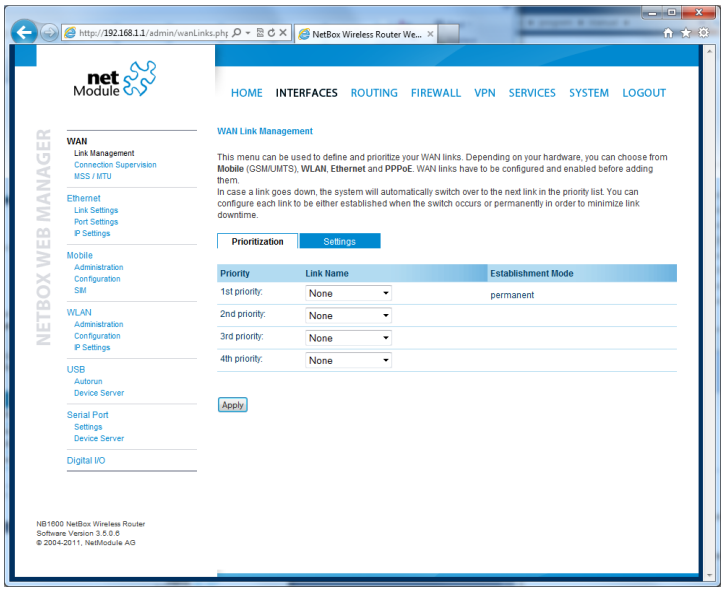
This menu can be used to define and prioritize your WAN links. Depending on your hardware, you can choose from **Mobile** (GSM/UMTS), **WLAN**, **Ethernet** and **PPPoE**. WAN links have to be configured and enabled before adding them.

In case a link goes down, the system will automatically switch over to the next link in the priority list. You can configure each link to be either established when the switch occurs or permanently in order to minimize link downtime.

Parameter	Description
1st priority:	This link will be used whenever ever possible.
2nd priority:	The first fallback link. It can be enabled permanently or at the point of time when Link 1 goes down.
3rd priority:	The second fallback technology. It can be enabled permanently or at the point of time when Link 2 goes down.
4th priority:	The third fallback technology. It can be enabled permanently or at the point of time when Link 3 goes down.

The switch-over behaviour can be refined with the following settings.

Parameter	Description
Mobile:	The required signal strength for GSM/UMTS in order to qualify the link as a fallback alternative. The link will not be dialled if the signal is below the configured threshold.
WLAN:	The required signal strength for WLAN in order to qualify the link as a fallback alternative. The link will not be dialled if the signal is below the configured threshold.

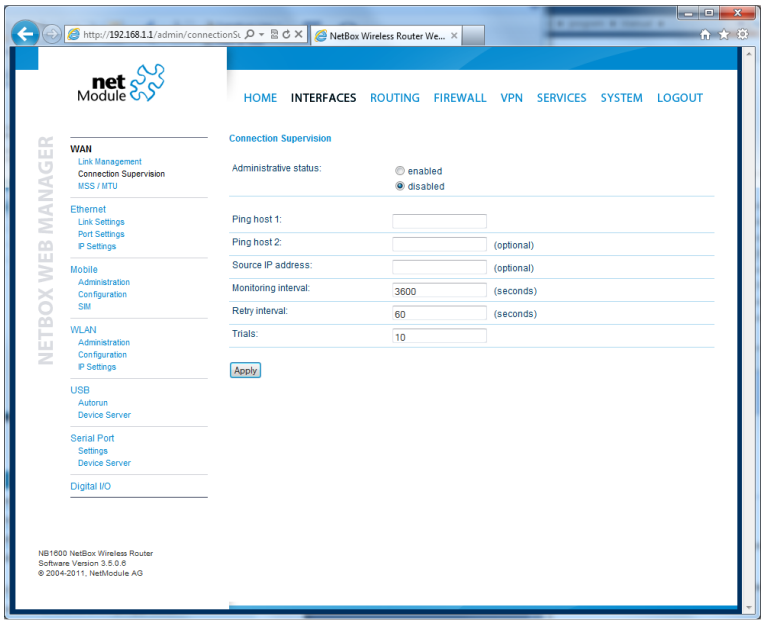


4.3.2.2 Connection Supervision

Parameter	Description
Supervision status:	Enable or disable connection supervision
Supervision method:	Currently only ICMP based ping supervision is supported.
Reference host 1:	Reference host 1 which will be used for checking IP connectivity (done via ICMP pings).
Reference host 2:	Reference host which will be used for checking IP connectivity (done via ICMP pings). The test is considered successful if either host 1 or 2 answers.
Source IP address:	IP address to be used as source of the ping probes. You can apply a specific interface address to force the usage of a particular link.
Monitoring interval:	The time to wait before sending the next probe (in case the last probe was successful).
Retry interval:	The time to wait until sending the next probe (in case the last probe was unsuccessful)l.
Trials:	Number of consecutive unsuccessful probes that are required until a recovery action is initiated.

The recovery actions are:

- Trying to re-establish a broken connection
- Restart the internal modem
- Restart the system


http://192.168.1.1/admin/connectionS
NetBox Wireless Router We...
net Module
HOME INTERFACES ROUTING FIREWALL VPN SERVICES SYSTEM LOGOUT
NETBOX WEB MANAGER
WAN
Link Management
Connection Supervision
MSS / MTU
Ethernet
Link Settings
Port Settings
IP Settings
Mobile
Administration
Configuration
SIM
WLAN
Administration
Configuration
IP Settings
USB
Autorun
Device Server
Serial Port
Settings
Device Server
Digital I/O
NB1600 NetBox Wireless Router
Software Version 3.5.0.6
© 2004-2011, NetModule AG
Connection Supervision
Administrative status:
enabled
disabled
Ping host 1:
Ping host 2:
(optional)
Source IP address:
(optional)
Monitoring interval:
3600
(seconds)
Retry interval:
60
(seconds)
Trials:
10
Apply

4.3.2.3 MSS / MTU

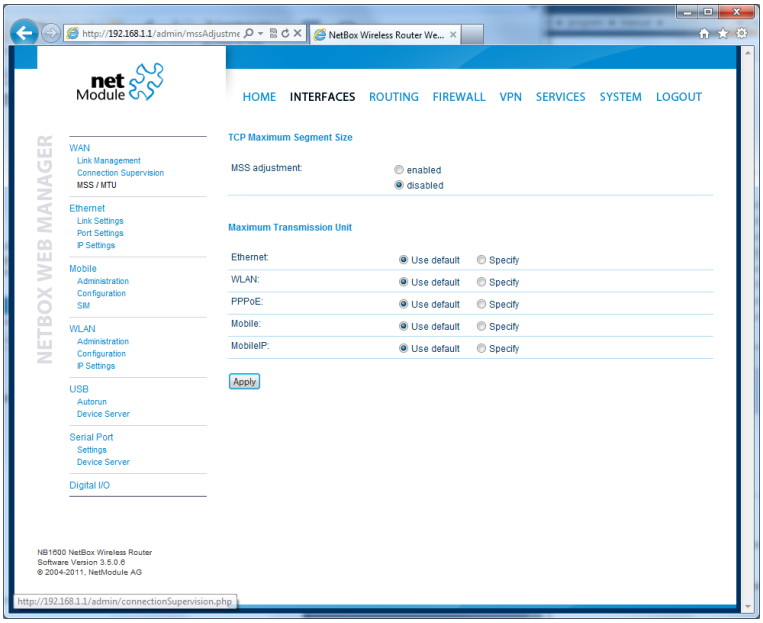
TCP Maximum Segment Size

The maximum segment size (MSS) is the largest amount of data, specified in bytes, that a computer or communications device can handle in a single, unfragmented TCP segment. For optimum communications, the number of bytes in the data segment and the headers must not add up to more than the number of bytes in the maximum transmission unit (MTU).

Parameter	Description
MSS adjustment:	Enable or disable MSS adjustment on WAN interfaces.
Maximum segment size:	Maximum number of bytes in a TCP data segment.

Maximum Transmission Unit

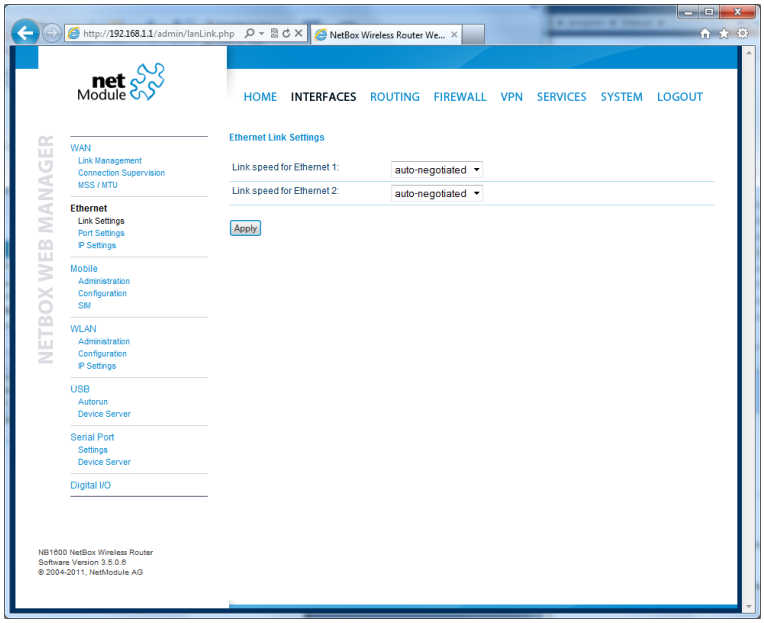
The Maximum Transmission Unit represents the largest amount of data that can be transmitted within one IP packet and can be defined for any WAN interface.



4.3.3 Ethernet

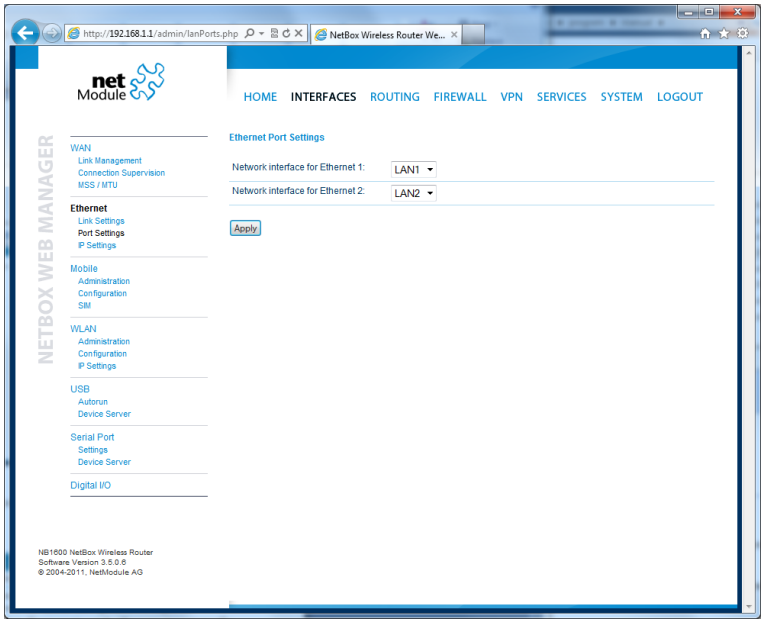
4.3.3.1 Link Settings

The link negotiation can be set for each Ethernet port individually. Most devices support auto-negotiation which will configure the link speed automatically according to the existing devices in the network



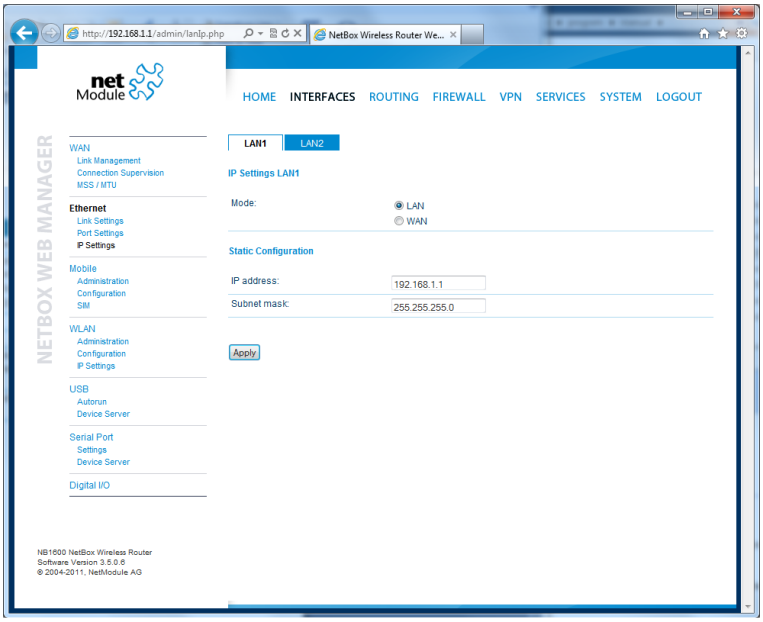
4.3.3.2 Port Settings:

This menu can be used to individually assign each Ethernet port to a LAN interface in case you want to have different subnets per port or use one port as WAN interface. If it is desired to have both ports in the same LAN you may assign them to the same interface. Please note that the ports will be bridged by software and operated by running the Spanning Tree Protocol.



4.3.3.3 IP Settings

Parameter	Description
Mode:	Define whether this interface is being used for LAN or WAN.
WAN mode:	**DHCP client** means that the IP configuration will be retrieved from a DHCP server in the network. Thus, no further configuration is required. **Static configuration** allows you to set the IP parameters manually. **PPPoE** is the preferred protocol when communicating with another WAN access device (like a DSL modem).
User name:	PPPoE user name to be used for authenticating at the access device.
Password:	PPPoE password to be used for authenticating at the access device.
Service name:	Specifies the service name set of the access concentrator. Leave it blank unless you have many services and need to specify the one you need to connect to.
Access concentrator name:	This may be left blank and the client will connect to any access concentrator.



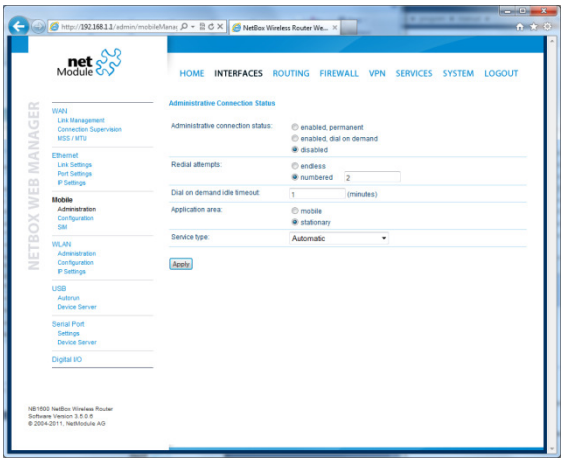
4.3.4 Mobile (2G, 3G, 3G+, 4G)

1. For setting up a Mobile connection, it's always a good idea to proceed as follows: Verify the card status in the SIM section and enter your PIN code in case your SIM card is using PIN protection.
2. Configure your provider's settings (such as user, password, APN) in the Configuration section. You can load these settings from our comprehensive database.
3. Enable the link in the Administration section, commonly with the default settings provided there.
4. Ensure to have the Mobile link set in WAN Link Management menu. Being the first WAN link, the primary link will automatically switch to Mobile then.

4.3.4.1 Administration

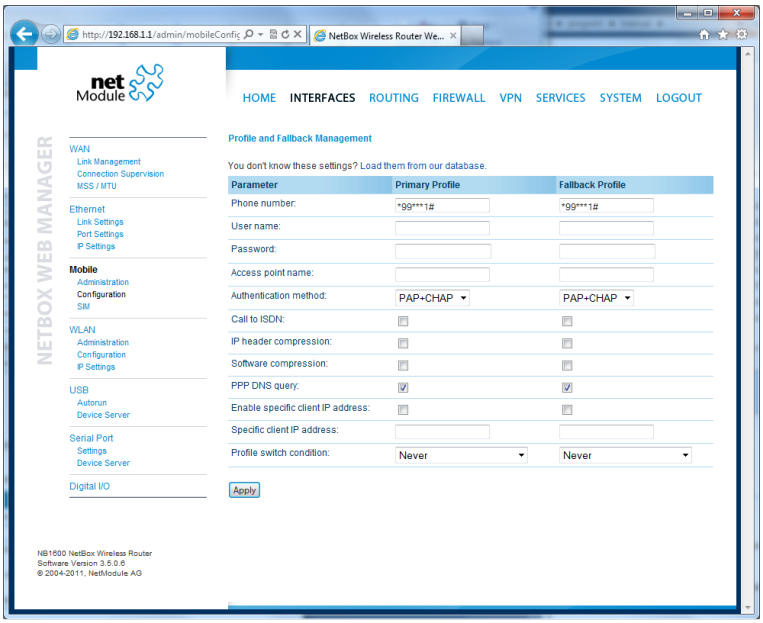
You can enable and disable the Mobile connection here and control the start mode of the Mobile link. Regarding the administrative status, we recommend using the 'permanent' option for unlimited accounts. Generally, the service type of the connection will be determined automatically depending on your coverage and general availability of networks like 3G+/4G. The UMTS/GSM LED will be blinking during the connection establishment process and goes on as soon as the connection is up. Refer to the troubleshooting section and log files if the connection does not come up.

Parameter	Description
Administrative connection status:	This can be permanent, dial on demand or disabled. On-demand links will be established as soon as outbound packets are routed to this interface. The permanent method will up the mobile interface permanently. In case of a disconnect or any link loss the connection will be re-established by the WAN link manager.
Redial attempts:	Number of redialling attempts prior to switching to the next profile.
Dial on demand idle timeout:	Time in minutes after an on-demand connection will be disconnected.
Operational connection status:	Shows whether the connection is up or not.
Application area:	You can define your application area here which is either mobile or stationary. Roaming or moving applications are often affected by coverage outage and dead spots the system therefore applies optimizations for stabilising the link.
Service type:	A fixed service type can be set here for instance to bypass any flapping issues between different networks.



4.3.4.2 Configuration

Parameter	Description
Phone number:	The phone number being dialled. Packet-switched connections for services like GPRS/UMTS usually use *99***1# for initializing the modem. For circuit-switched connections you can enter the fixed phone number to dial in international format (e.g. +41xx).
User Name:	The username provided by your provider or mobile operator (can be empty)
Password:	The password provided by your provider (can be empty)
Access point name:	The Access Point Name, provided by your provider (may depend on your account). In general, you can find it in our database.
Authentication method:	Use Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP)
Call to ISDN:	Has to be enabled if the connection is talking to an ISDN modem.
IP Header Compression:	Enable or disable Van Jacobson TCP/IP Header Compression for PPP. This feature will improve TCP/IP performance over slow serial links. Has to be supported by your provider.
Software Compression:	Enable or disable PPP data compression. Software compression reduces the size of PPP packets to improve throughput. Has to be supported by your provider.
PPP DNS query:	Being enabled, the DNS servers are negotiated during PPP connection establishment.
Enable Specific Client IP Address:	Enable or disable a fixed IP address on the mobile interface
Specific Client IP Address:	Specify a fixed client IP address on the mobile interface.
Profile switch condition:	Specifies the condition for a profile switch to the other profile.



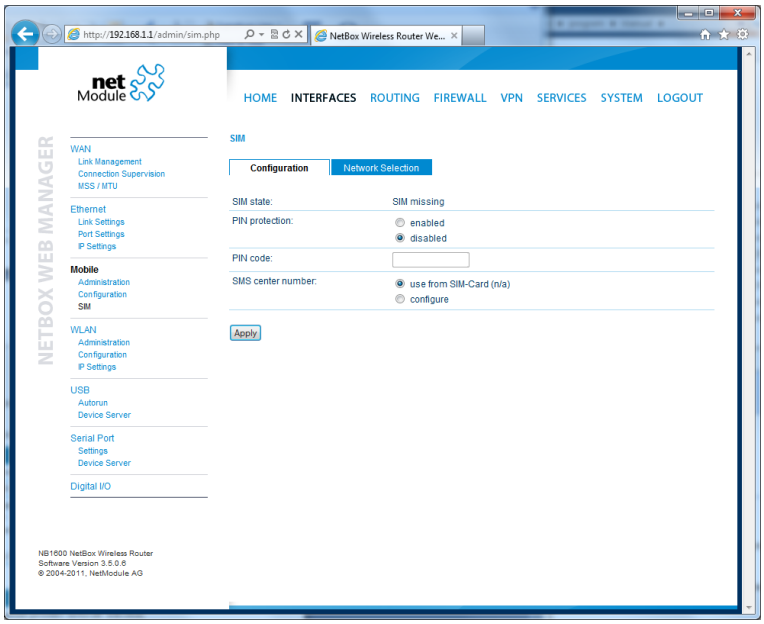
4.3.4.3 SIM

This section can be used to configure your PIN code and SIM settings. PIN protection can only be changed if you entered a correct PIN code before.

NetBox can only handle SIM cards if either the correct PIN code is provided or if PIN protection is disabled.

Parameter	Description
PIN protection:	Enable or disable PIN protection
PIN code:	The PIN code for the SIM card
SMS center number:	Number of Short Message Service Centre (SMSC) for sending Mobile Originating (MO) SMS messages Contact your mobile operator for obtaining the correct number. A comprehensive database can also be found here: http://umtslink.at/sms/smsc_rufnummern.htm

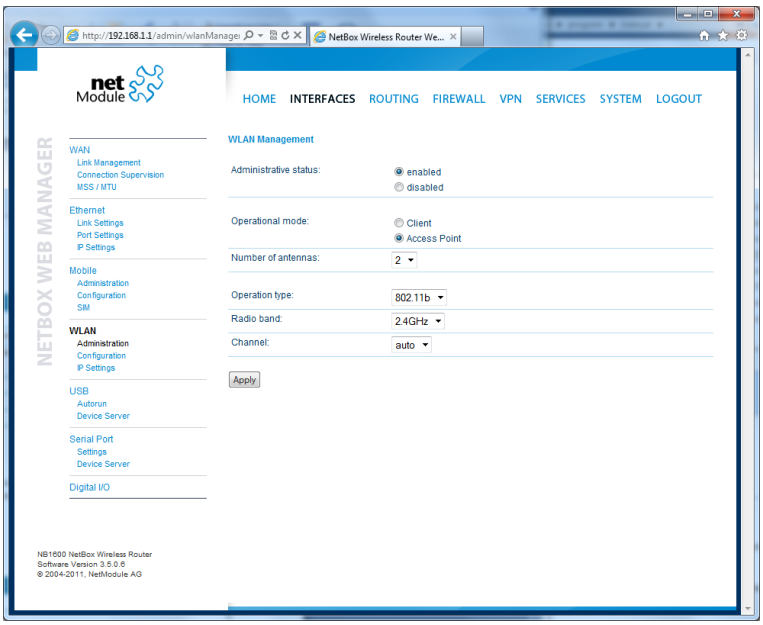
Parameter	Description
Network selection:	Choose between automatic or manual provider network selections. For manual selection you will need to specify the provider.



4.3.5 WLAN

4.3.5.1 WLAN Administration

Parameter	Description
Administrative status:	Enable or disable WLAN.
Operational mode:	Choose whether the WLAN card should operate in access point or client mode.
Number of antennas:	Configure the number of attached WLAN antennas. At least one antenna must be attached to WLAN 1. We generally recommend using a second antenna for better coverage and throughput. For higher throughput rates in 802.11n a second antenna is mandatory.
Operation type:	You can specify the desired type of IEE 802.11 operation. 802.11a can be used in the 5 GHz band, higher throughput in 20/40 MHz mode can be achieved in 802.11n.
Radio band:	Select the band to be used (depends on your WLAN module).
Channel:	The channel to be used. If automatic is selected, the system will automatically scan your neighbouring networks and choose the less interfering channel according to your configuration.

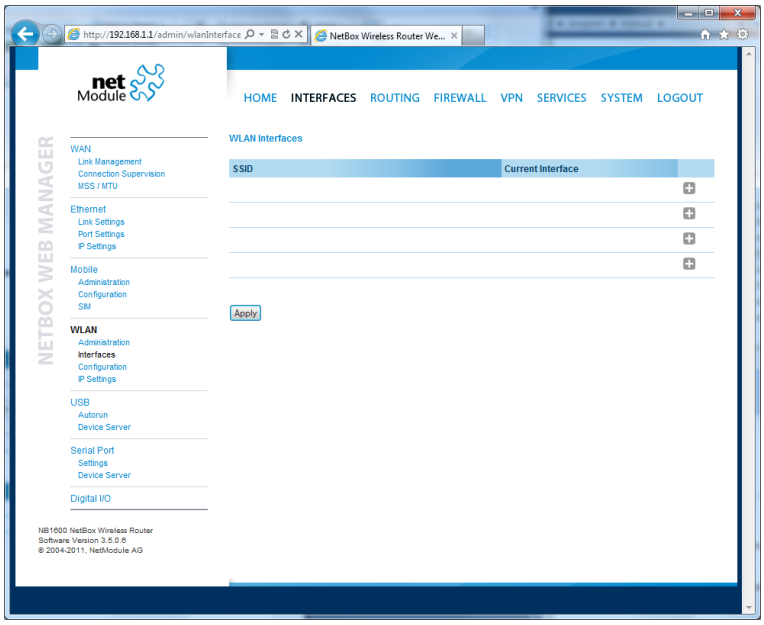


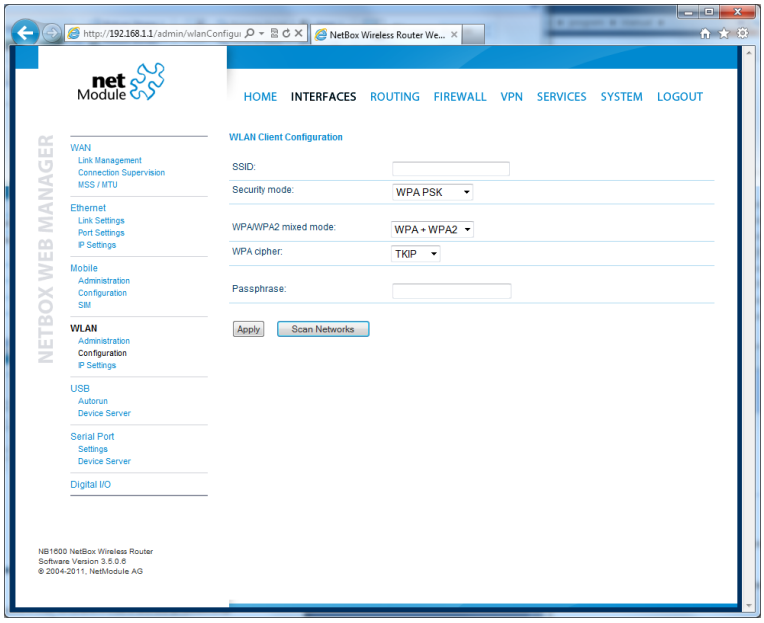
4.3.5.2 WLAN Configuration

The WLAN interface can be operated in client- or access-point mode. In client-mode, it can be used as an additional WAN link and added to the WAN Link Management In access-point mode you can define up to 4 networks being offered. The networks can be individually bridged to a LAN interface or operate as dedicated interfaces in routing-mode.

4.3.5.3 WLAN Configuration Client

Running in client-mode you can select the network to which you want to connect to and enter the required authentication settings. You may also perform a WLAN network scan and pick the settings from the discovered information directly. The credentials can be obtained by the administrator of your WLAN access point.





4.3.5.4 WLAN Configuration Access Point

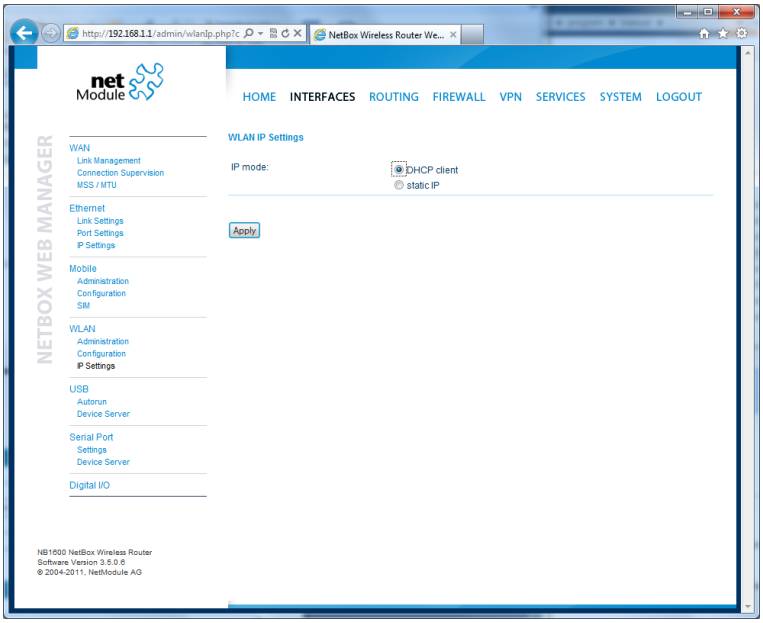
Running in access-point mode you can define up to 4 SSIDs that is networks to be broadcasted to your WLAN clients. This section can be used to configure security related features.

Parameter	Description
SSID:	The network name (SSID).
Security mode:	The desired security mode. We strongly recommend performing authentication and encryption on any WLAN links such as WPA PSK. WPA (802.1x) can be used to authenticate against a remote RADIUS server in your backbone. A RADIUS server can be configured in the Remote Authentication section.
WPA/WPA2 mixed mode:	WPA2 should be preferred over WPA1. Running WPA/WPA2 mixed mode offers both.
WPA cipher:	The WPA cipher to be used, you can leave both TKIP + CCMP.
Passphrase:	Your passphrase

4.3.5.5 WLAN IP Settings

This section can be used to configure the TCP/IP settings of your WLAN networks when running in access-point mode. You can bridge the WLAN interface to any LAN interface for letting WLAN clients and LAN hosts operating in the same subnet. However, for multiple SSIDs we strongly recommend to set up the networks in routing-mode separately in order to avoid unwanted access and traffic between the interfaces. You can configure a dedicated DHCP server on each network in the DHCP Server section.

Parameter	Description
Network mode:	Choose between bridged or routed mode.
Bridge interface:	You can specify the LAN interface here to which the network should be bridged.
IP address / netmask:	Configure the IP address and netmask for this WLAN interface.



Running in client-mode, you can specify here whether you want to obtain your IP address automatically via DHCP, you may also configure a fixed address if you want to bypass DHCP negotiation.

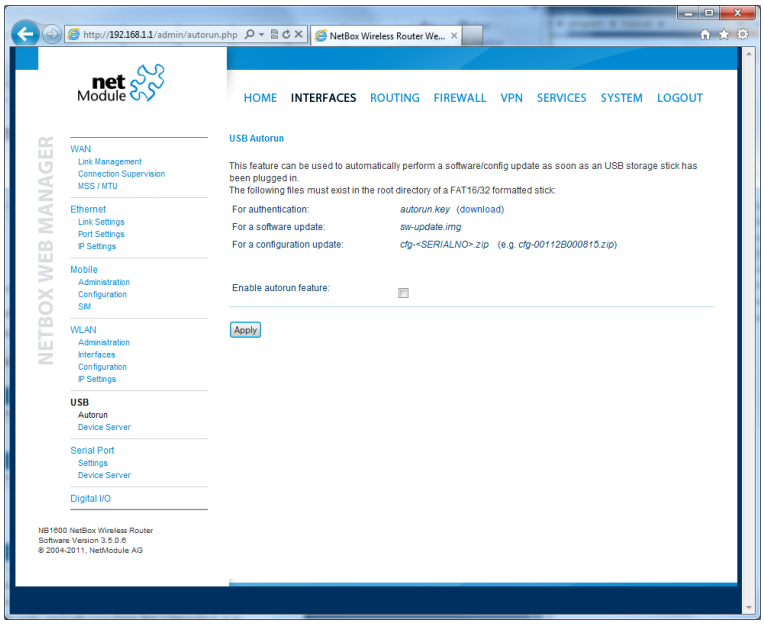
4.3.6 USB Port

4.3.6.1 USB Autorun

This feature can be used to automatically perform a software/config update as soon as an USB storage stick has been plugged in.
The following files must exist in the root directory of a FAT16/32 formatted stick:

- For authentication: autorun.key
- For a software update: sw-update.img
- For a configuration update: cfg-<SERIALNO>.zip (e.g. cfg-00112B000815.zip)

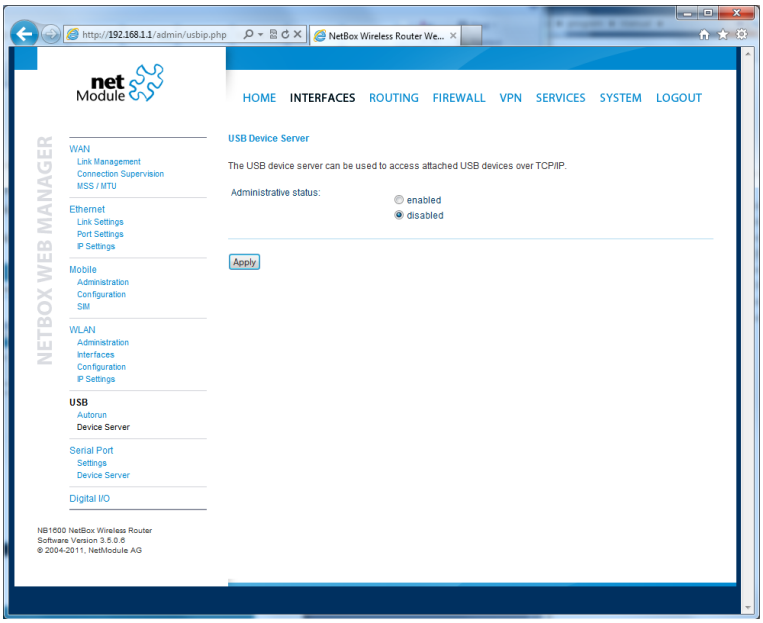
Parameter	Description
Enable auto run feature:	Enable or disable auto run feature.



The autorun.key file must hold valid access keys to perform any actions when the storage device is plugged in. The keys are made up of your admin password. They can be generated and downloaded. You may also define multiple keys in this file (line-after-line) in case your admin password differs if applied to multiple NetBox routers.

4.3.6.2 USB Device Server

Parameter	Description
Administrative status:	Enable or disable USB device server.

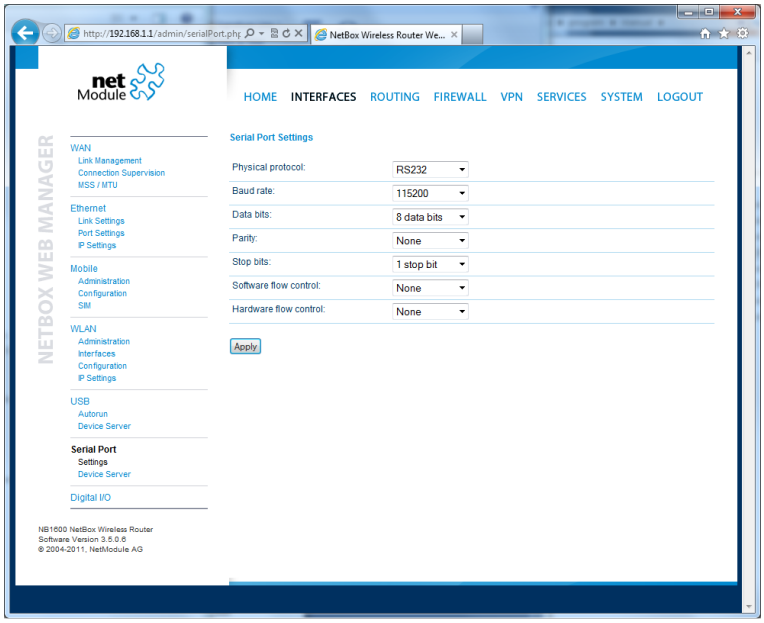


As soon as the USB device server has been enabled you can refresh the discovered USB devices plugged in and attach them to the USB/IP server. Enabled device can now be exported to a remote host. You will need an additional driver on the remote site and further installation instructions which we will happily provide on demand.

4.3.7 Serial Port

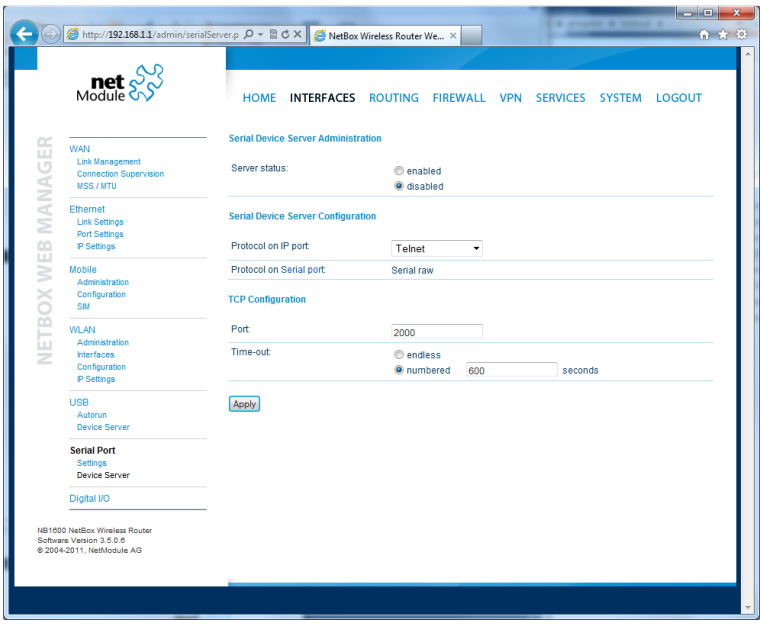
4.3.7.1 Serial Port Settings

Parameter	Description
Physical protocol:	NB1600 currently only supports RS232.
Baud rate:	This property specifies the baud rate of the COM port
Data bits:	This property specifies the number of data bits contained in each frame.
Parity:	This property specifies the parity used with every frame that is transmitted or received.
Stop bits:	This property specifies the number of stop bits used to indicate the end of a frame.
Software support	In XON/XOFF software flow control, either end can send a stop (XOFF) or start (XON) character to the other end to control the rate of incoming data.
Hardware flow control	In RTS/CTS hardware flow control, the computer and the modem use the RTS and CTS lines respectively to control the flow of data



4.3.7.2 Serial Device Server

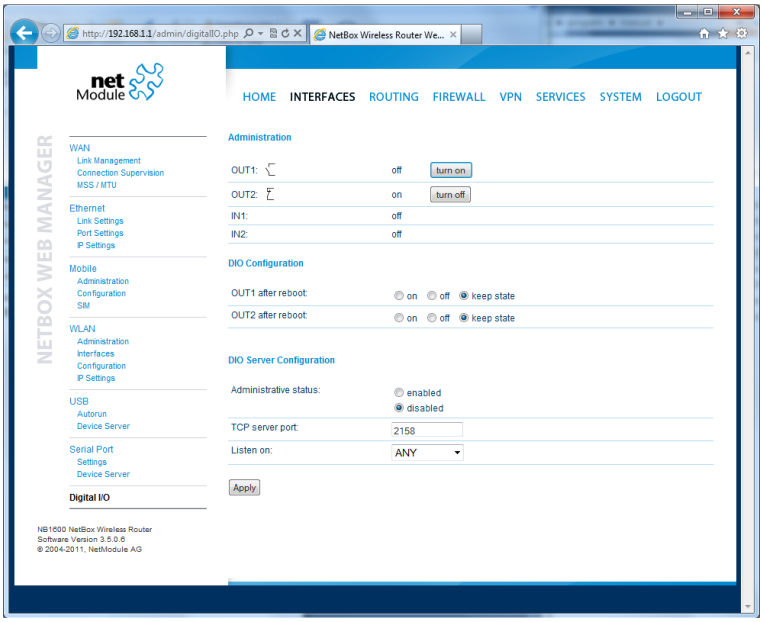
Parameter	Description
Server status:	Enable or disable serial device server.
Protocol on TCP/IP:	“Telnet” or “TCP raw”
Protocol on serial port:	The protocol implicitly defined on the serial port.
Port:	The TCP port that is used by this application.
Time-out:	Time-out.



4.3.8 Digital I/O

Parameter	Description
OUT1 after reboot:	Initial status of OUT1 after the system has booted.
OUT2 after reboot:	Initial status of OUT2 after the system has booted.
Administrative status:	Enable or disable the Digital I/O management server.
TCP server port:	TCP port of the Digital I/O management server.
Listen on:	Specify the interface where the I/O monitor shall be accessible.

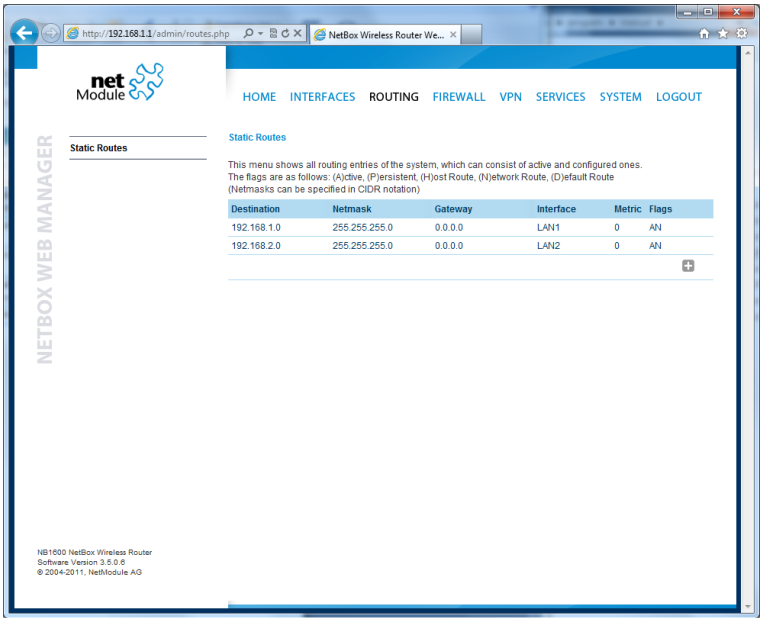
The digital inputs and outputs can be monitored and controlled via the Web Manager or by software. See section 6.1 (Digital I/O Server) on how to control inputs and outputs by software.



4.4 Routing

This menu shows all routing entries of the system, which can consist of active and configured ones. (Netmasks can be specified in CIDR notation, i.e. **/24** expands to **255.255.255.0**).

Parameter	Description
Destination	The destination network or host provided by IP addresses in dotted decimal.
Netmask	The subnet mask which forms, in combination with the destination, the network to be addressed. A single host can be specified by a netmask of 255.255.255.255, a default route corresponds to 0.0.0.0.
Gateway	The next hop which operates as gateway for this network (can be omitted on peer-to-peer links).
Interface	The network interface on which a packet will be transmitted in order to reach the gateway or network behind.
Metric	The routing metric of the interface (default 0). The routing metric is used by routing protocols, higher metrics have the effect of making a route less favourable; metrics are counted as additional costs to the destination network.
Flags	(A)ctive, (P)ersistent, (H)ost Route, (N)etwork Route, (D)efault Route


http://192.168.1.1/admin/routes.php
NetBox Wireless Router We...
net Module
HOME INTERFACES ROUTING FIREWALL VPN SERVICES SYSTEM LOGOUT
NETBOX WEB MANAGER
Static Routes
Static Routes
This menu shows all routing entries of the system, which can consist of active and configured ones.
The flags are as follows: (A)ctive, (P)ersistent, (H)ost Route, (N)etwork Route, (D)efault Route
(Netmasks can be specified in CIDR notation)
Destination Netmask Gateway Interface Metric Flags
192.168.1.0 255.255.255.0 0.0.0.0 LAN1 0 AN
192.168.2.0 255.255.255.0 0.0.0.0 LAN2 0 AN
NB1600 NetBox Wireless Router
Software Version 3.5.0.6
© 2004-2011, NetModule AG

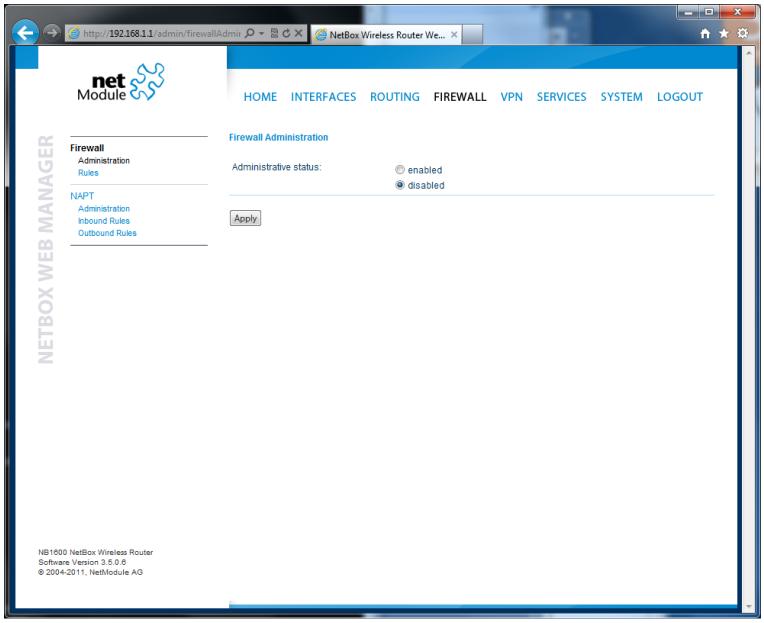
4.5 Firewall

This router uses Linux's netfilter/iptables firewall framework (see http://www.netfilter.org for more information). It is set up of a range of rules which control each packet's permission to pass the router. Packets, not matching any of the rules, are per default allowed.

4.5.1 Firewall Administration and Rules

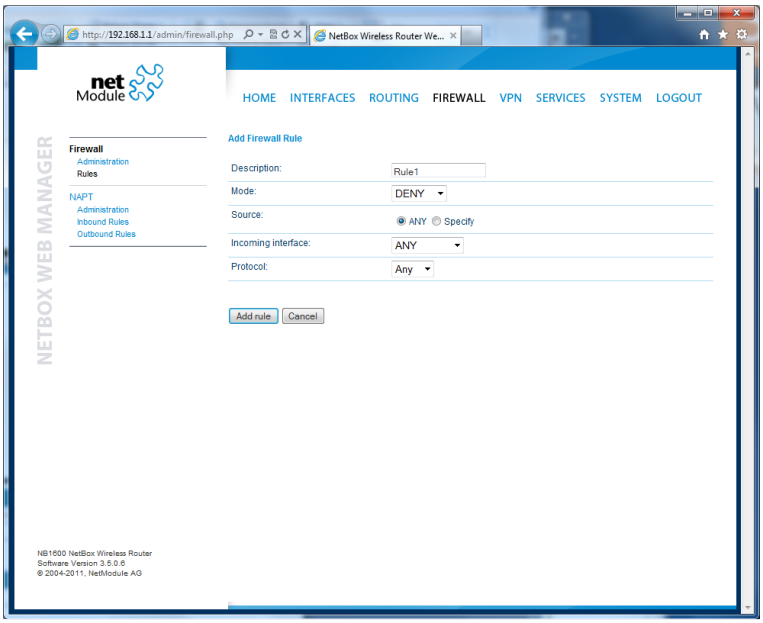
4.5.1.1 Firewall Administration / Rules

Parameter	Description
Administrative status:	Enable or disable packet filtering.
Enable WAN access:	This shortcut will create rules for allowing access to the management services on the WAN link.



4.5.1.2 Firewall Rules

Parameter	Description
Description:	A meaningful description about the purpose of this rule.
Mode	Whether the packets of this rule should be allowed or denied.
Source:	The source address of matching packets, can be any or a source network/host.
Incoming interface:	The interface on which matching packets are received.
Protocol:	The used IP protocol of matching packets.
Destination port(s):	The destination port of matching packets. You can specify a single port or a range of ports here. Note that protocol must be set to UDP/TCP when using port filters.

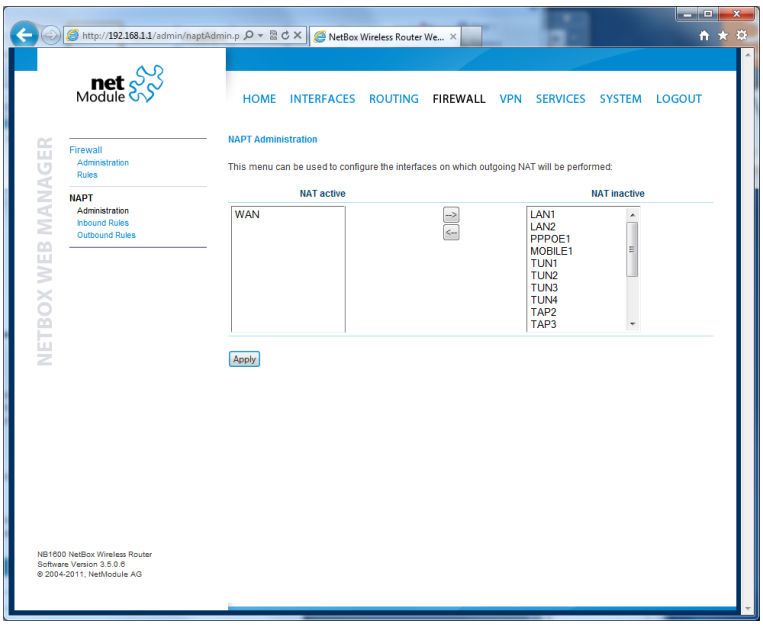


4.5.2 NAPT

This page lets you set the options for Network Address and Port Translation (NAPT). NAPT translates IP addresses or TCP/UDP ports and enables communication between hosts on a private network and hosts on a public network. It generally allows a single public IP address to be used by many hosts from the private LAN network.

4.5.2.1 NAPT Administration

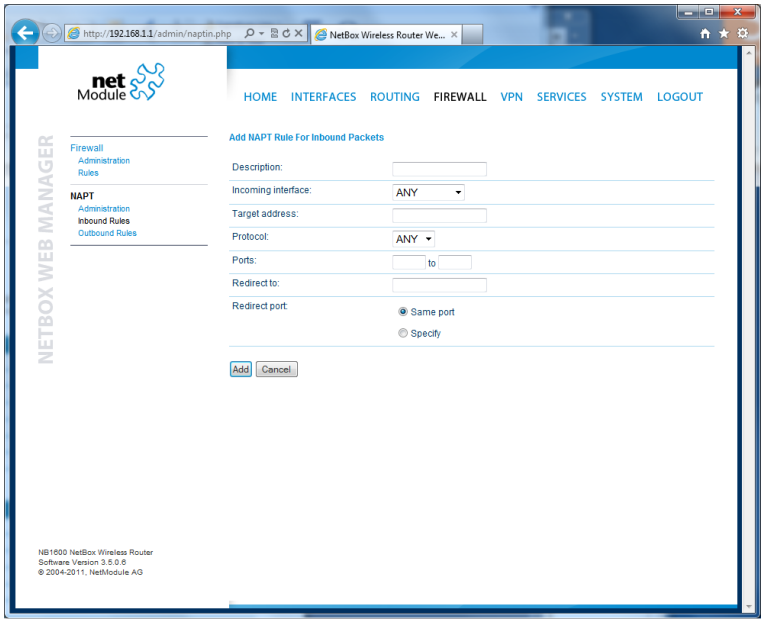
This menu can be used to configure the interfaces on which outgoing NAT will be performed



4.5.2.2 NAPT Inbound Rules

Inbound rules can be used to modify the target section of IP packets and, for instance, forward a service or port to an internal host. By doing so, they will expose the service and make it reachable e.g. from the Internet. You may also establish 1:1 NAT to a complete host.

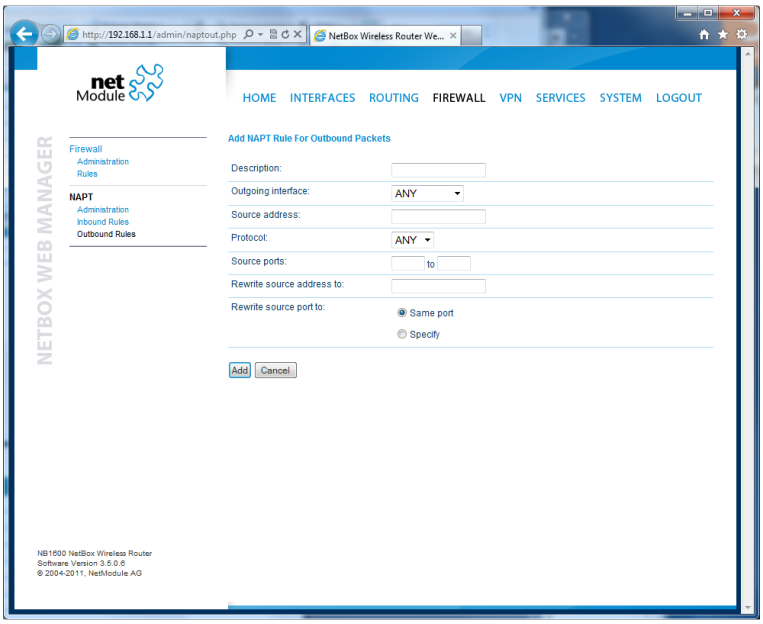
Parameter	Description
Description	A meaningful description of this rule
Incoming interface:	The interface from which matching packets are received
Target address:	The destination address of matching packets (optional)
Protocol:	The used protocol of matching packets
Ports:	The used UDP/TCP port of matching packets
Redirect to:	The address to which matching packets shall be redirected
Redirect port:	The port to which matching packets will be targeted.



4.5.2.3 NAPT Outbound Rules

Outbound rules will modify the source section of IP packets and can be for instance used for 1:1 NAT.

Parameter	Description
Description	A meaningful description of this rule
Incoming interface:	The outgoing interface on which matching packets are leaving the router
Source address:	The source address of matching packets (optional)
Protocol:	The used protocol of matching packets
Ports:	The used UDP/TCP port of matching packets
Rewrite source address:	The address to which the source address of matching packets shall be rewritten
Rewrite source port:	The port to which the source port of matching packets shall be rewritten

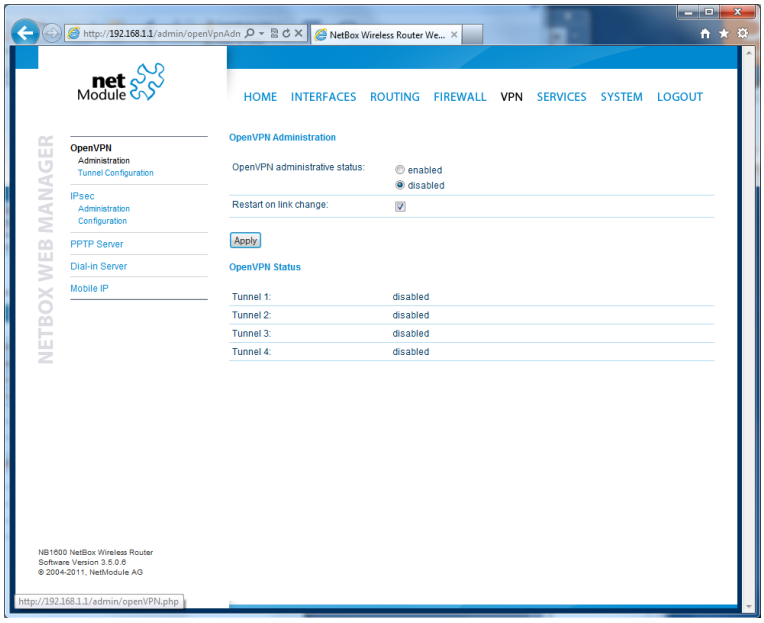


4.6 VPN

4.6.1 OpenVPN

4.6.1.1 OpenVPN Administration

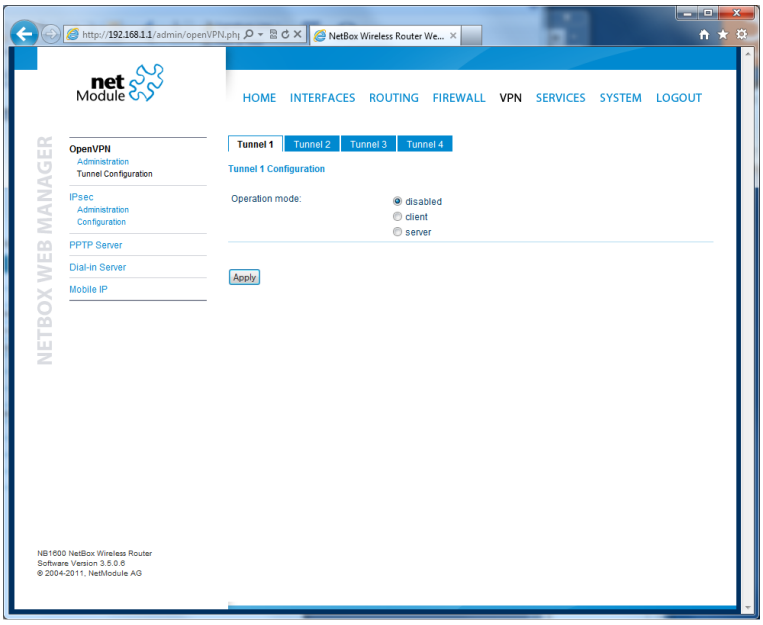
Parameter	Description
OpenVPN administrative status:	Enable or disable OpenVPN. If enabled, OpenVPN client configurations will be started whenever a WAN link has been established. Server configurations will be started immediately after boot up.



4.6.1.2 OpenVPN Tunnel Configuration

The router supports a single server tunnel and up to 4 client tunnels. You can specify tunnel parameters in standard configuration or upload an expert mode file which has been created in advance. Refer to section 'OpenVPN Client Management' to learn more about how to manage clients and generate the files.

Parameter	Description
Operation mode:	Choose client or server mode for this tunnel
Primary server address:	Primary OpenVPN server address (for clients)
Primary server port:	The OpenVPN server port (1194 by default)
Secondary server address:	Secondary OpenVPN server address (optional, for clients) to switch over in case the primary address cannot be reached
Secondary server port:	Secondary OpenVPN server port (optional, for clients)
Type	The VPN device type which can be either TUN (typically used for routed connections) or TAP (used for bridged networks)
Network mode:	Defines how the packets should be forwarded, can be routed or bridged from or to a particular interface.
Cipher:	The required cipher mechanism used for encryption.
Use compression:	Enable or disable OpenVPN compression
Use keep alive:	Can be used to send a periodic keep alive packet in order to keep the tunnel up despite of inactivity.
Redirect gateway:	By redirecting the gateway, all packets will be directed to the VPN tunnel. Please ensure that essential services (such as DNS or NTP servers) can be reached at the network behind the tunnel. In doubt, create an extra static route pointing to the correct interface.
Protocol:	The OpenVPN tunnel protocol to be used.
Authentication:	You can choose between no authentication, credential-based (where you have to specify a username and password) and based on keys and certificates. Note that keys/certificates have to be created under SYSTEM -> Keys/Certificates. You may also uploaded files which you have generated on your host system.



4.6.1.3 OpenVPN Expert Configuration (Client)

The expert configuration mode offers a straightforward way to configure a tunnel by simply uploading a package containing the required configuration and key/certificate file. For a client tunnel the typical files are:

- client.conf (OpenVPN configuration file, see http://www.openvpn.net for available options)
- ca.crt (root certificate file)
- client.crt (certificate file)
- client.key (private key file)

Please note, that you may specify arbitrary file names, however, the configuration file suffix must be .conf and all files referred in the conf must correspond relatively to the path names specified in the configuration.

4.6.1.4 OpenVPN Expert Configuration (Server)

:

A server tunnel typically requires the following files:

- server.conf (OpenVPN configuration file)
- ca.crt (root certificate file)
- server.crt (certificate file)
- server.key (private key file)
- dh1024.pem (Diffie hellman parameters file)
- a directory (with default name “ccd”) containing client-specific configuration files

Keep in mind that OpenVPN tunnels usually require a correct system time. Please ensure that all NTP servers are reachable. Using host names also required a working DNS server.

4.6.1.5 OpenVPN Client Management

Once you have successfully set up an OpenVPN server tunnel you can manage and enable clients which can connect to your service, the client’s page also informs you about currently connected clients. Further, you can specify a fixed tunnel endpoint address of each client and its network behind. You can also define routes to be pushed to each client if you want to redirect traffic for particular networks towards the server.

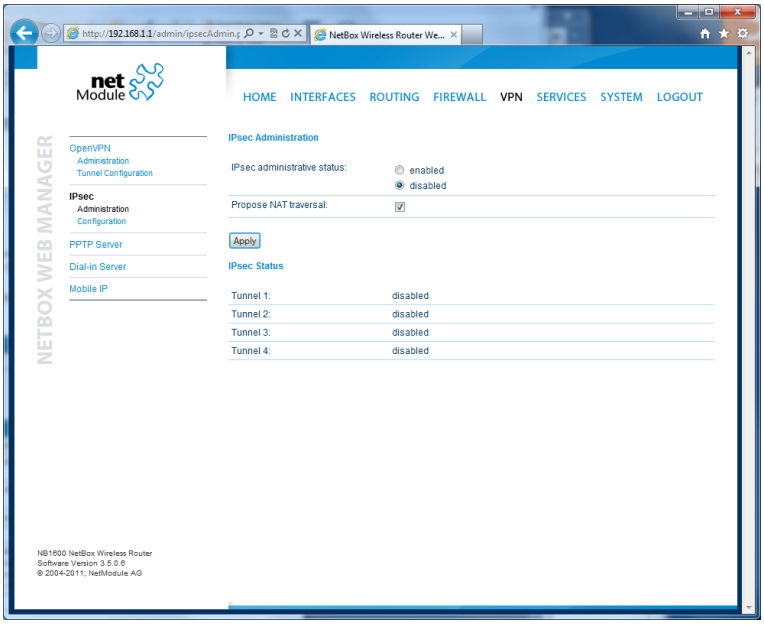
Finally, you can generate and download all expert mode files to easily populate each client.

4.6.2 IPsec

IPsec is primarily used for securing Internet communications by authenticating and/or encrypting IP packets within a data stream. IPsec includes various cryptographic protocols and ciphers for key exchange and data encryption and can be seen as one of the strongest VPN technologies in terms of security.

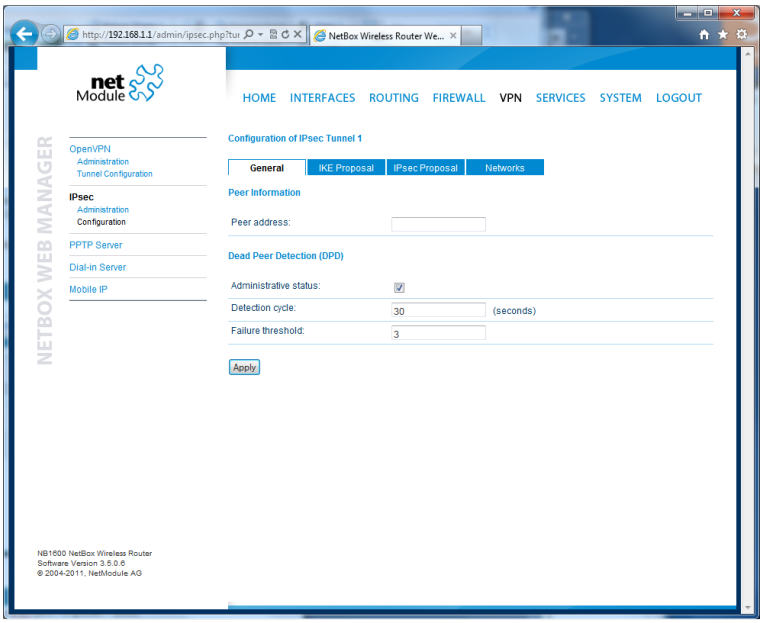
4.6.2.1 IPsec Administration

Parameter	Description
IPsec administrative status:	Enable or disable IPsec.



4.6.2.2 IPsec Configuration

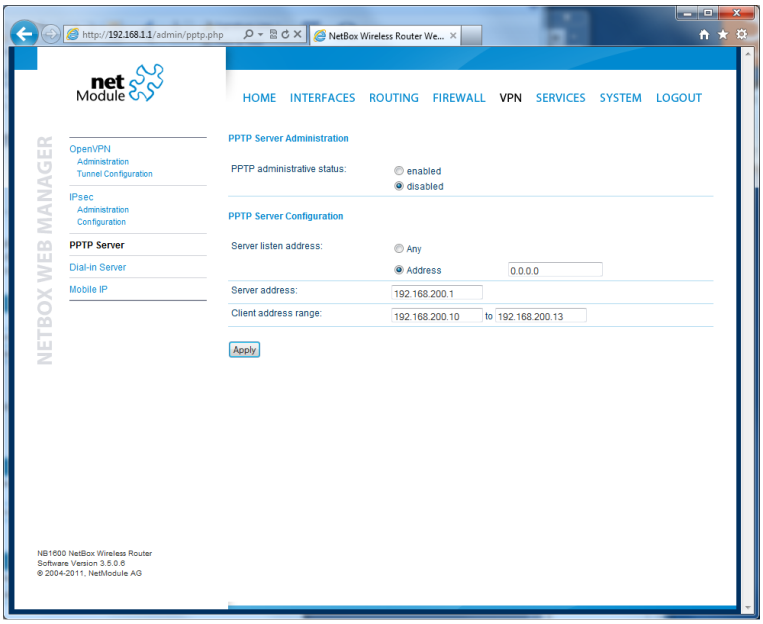
Parameter	Description
Remote server address:	IP address or host name of IPsec peer / responder / server.
Remote LAN address:	The remote private network, provided by an IP address in dotted decimal notation
Remote LAN subnet mask:	The remote private network, provided by a subnet mask in dotted decimal notation.
NAT Traversal	Enable or disable NAT-Traversal. NAT-Traversal is mainly used for connections which traverse a path where a router modifies the IP address/port of packets. It encapsulates packets in UDP and therefore requires a slight overhead which has to be taken into account when running over small-sized MTU interfaces.
Preshared Key (PSK):	The pre-shared key (PSK)
IKE mode:	Choose a negotiation mode. The default is main mode (identity-protection). Aggressive mode has to be used when dealing with dynamic endpoint addresses. It is however referred to be less secure compared to main mode as it reveals your identity to an eavesdropper.
IKE encryption:	IKE encryption method
IKE hash:	IKE hash method
IKE Diffie-Hellman Group:	IKE Diffie-Hellman Group
Perfect Forward Secrecy (PFS):	Use Perfect Forward Secrecy. This feature heavily increases security as PFS avoids penetration of the key-exchange protocol and prevents compromisation of keys negotiated earlier.
Local ID:	Local ID
Remote ID:	Remote ID
ESP encryption:	ESP encryption method
ESP hash:	ESP hash method
Status:	Enable or disable Dead Peer Detection. DPD will detect any broken IPSec connections, in particular the ISAKMP tunnel, and refresh the corresponding SAs (Security Associations) and SPIs (Security Payload Identifier) for a faster re-establishment of the tunnel.
Detection cycle [sec]:	Set the delay (in seconds) between Dead Peer Detection (RFC 3706) keep alives (R_U_THERE, R_U_THERE_ACK) that are sent for this connection (default 30 seconds).
Failure count:	The number of unanswered DPD R_U_THERE requests until the IPsec peer is considered dead (The router will then try to re-establish a dead connection automatically).



4.7 PPTP Server

The Point-to-Point Tunnelling Protocol (PPTP) is a method for implementing virtual private networks between two hosts. PPTP is easy to configure and widely deployed amongst Microsoft Dial-up networking servers. However, it is nowadays considered insecure. You will need to define users that are allowed to connect to the PPTP server in the 'User Accounts' section;

Parameter	Description
PPTP state	Enable/disable PPTP server
PPTP address range start:	Address range start for PPTP clients
PPTP address range size:	Address range size



4.8 Dial-in Server

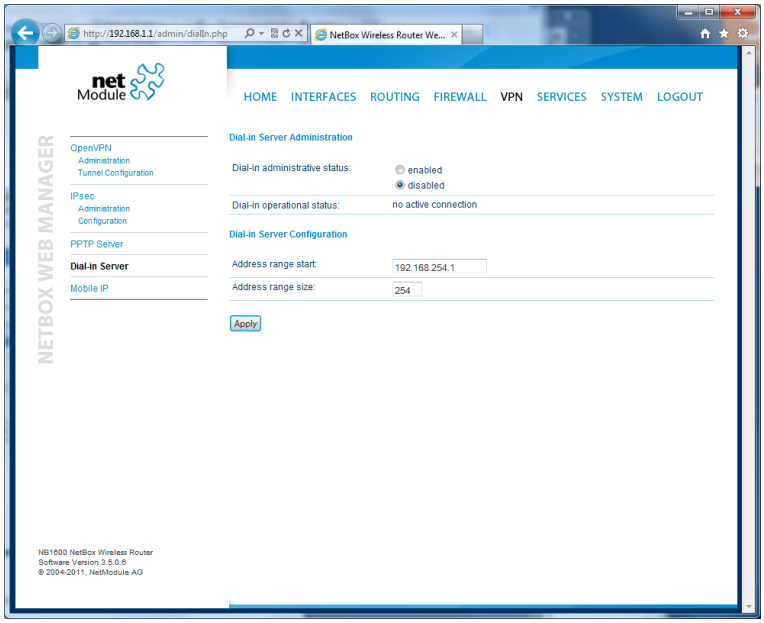
On this page you can configure the Dial-in server answering data calls over a mobile connection. Users that are allowed to dial-in are defined under the section “User Accounts”. Note that a concurrent use of Mobile Dial-Out and Dial-In is not possible. Also ensure that the service type must be set to ‘GSM only’ under INTERFACES -> Mobile -> Administration.

4.8.1 Dial-in Server Administration

Parameter	Description
Dial-in administrative status:	You can specify the administrative status whether incoming call shall be answered or not.
Dial-in operational status:	Shows whether a connection is active or not

4.8.2 Dial-in Server Configuration

Parameter	Description
Address range start:	Start address of range of clients connecting to the dial-in server.
Address range size:	Number of client addresses connecting to the server.

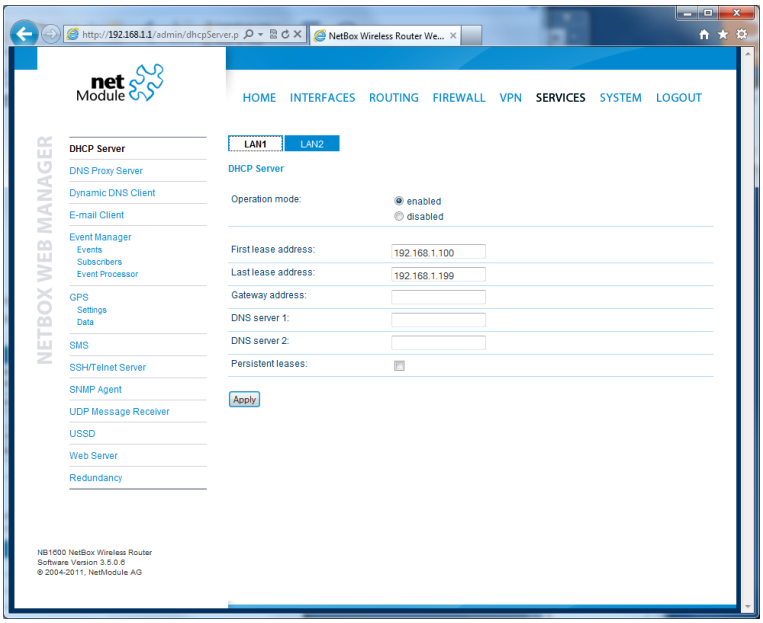


4.9 Services

4.9.1 DHCP Server

This section can be used to individually configure a DHCP service for each LAN interface.

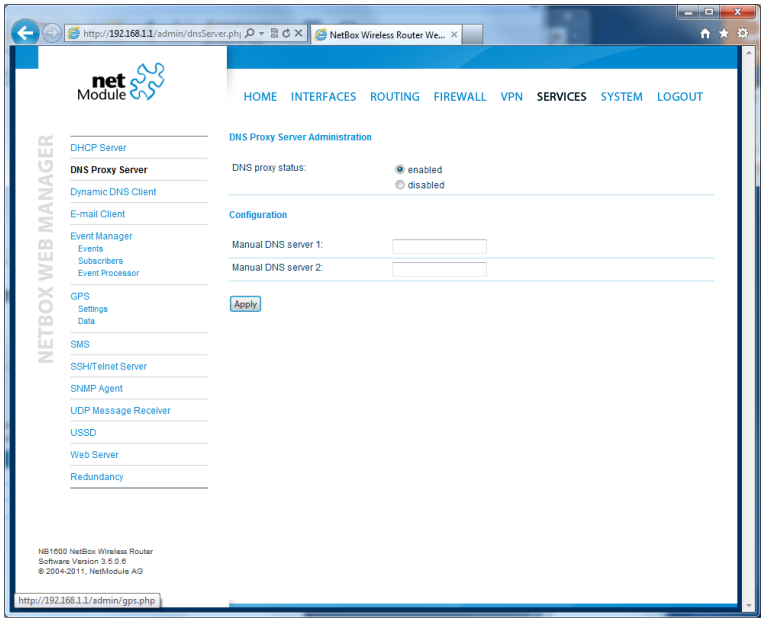
Parameter	Description
Operation mode:	The Dynamic Host Configuration Protocol (DHCP) server can be enabled or disabled. If enabled it will answer to DHCP requests from hosts in the LAN.
First lease address:	First address for DHCP clients
Last lease address:	Last address for DHCP clients.
DNS server 1:	Manually configured first DNS server (optional)
DNS server 2:	Manually configured second DNS server (optional)
Persistent leases:	By turning on this option the router will remember give leases even after a reboot which can be used to ensure the same IP addresses being assigned to a particular host.
DHCP options:	By default the DHCP will hand out the interface address as default gateway and DNS server address if not configured else wise. You can specify different addresses here.



4.9.2 DNS Proxy Server

The DNS Proxy is able to forward DNS requests to the DNS server provided during WAN link negotiation but also caching already resolved entries and thus reducing outbound DNS traffic. You may also specify static hosts for assigning fixed addresses to particular host names.

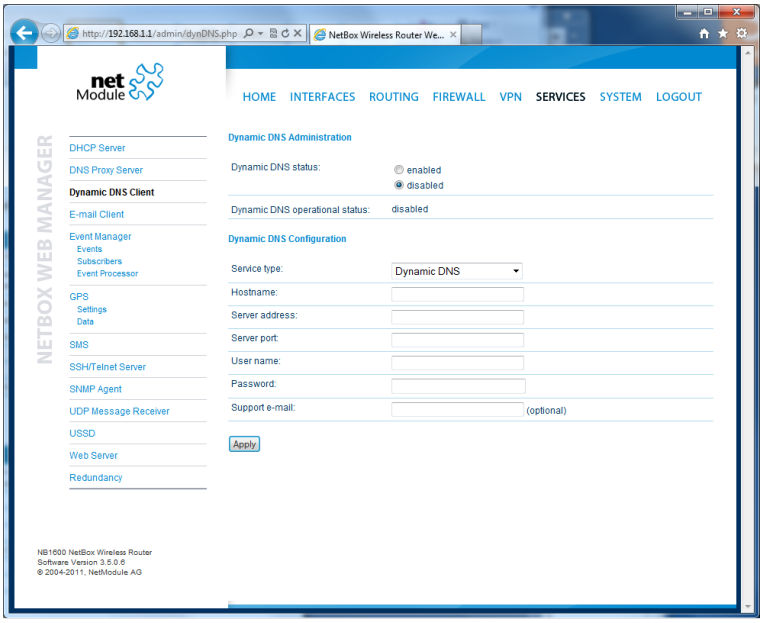
Parameter	Description
DNS proxy status:	Enabled or disabled
Manual DNS server 1:	The primary DNS server to be queried
Manual DNS server 2:	The secondary DNS server just in case the primary server is not available



4.9.3 Dynamic DNS

The dynamic DNS client on this box x is generally compatible to various DynDNS services in the Internet running by means of definitions by the DynDNS organization (see www.dyndns.com for server implementations).

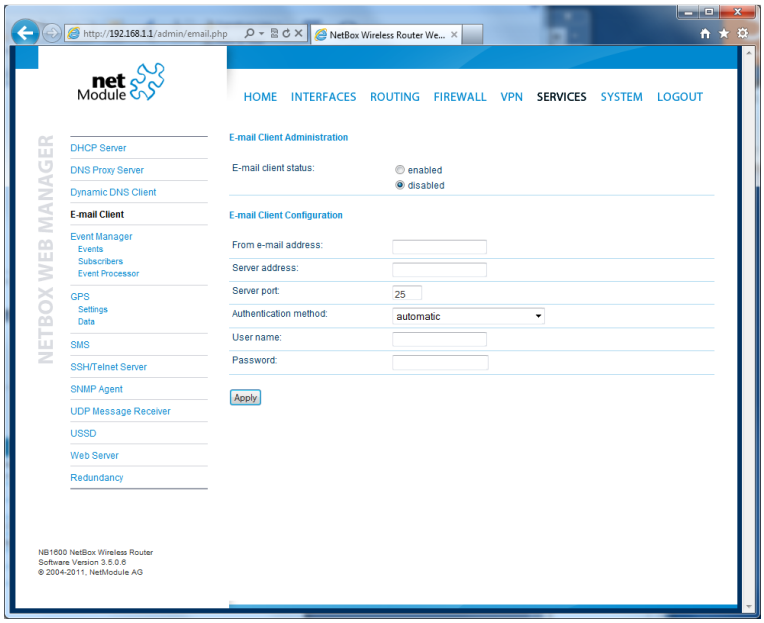
Parameter	Description
Dynamic DNS status:	Enable or disable the Dynamic DNS Client
Service type:	The DynDNS service type and protocol being used.
Host name:	The provided DynDNS name, e.g. mybox.dyndns.org
Server address:	Server IP address or host name(typically members.dyndns.org)
Server port:	Server port of the DynDNS server
User name:	Username used for authenticating at the service
Password:	Password used for authentication
Support e-mail:	Support e-mail address (required for some services)



4.9.4 E-mail Client

The E-Mail client can be used to send notifications to a particular E-Mail address upon certain events.

Parameter	Description
E-mail client status:	Administrative status of the E-Mail client
From e-mail address:	E-Mail address of the sender
Server address:	SMTP server address
Server port:	SMTP server port (typically 25)
Authentication method:	Choose the required authentication method which is used to authenticate against the SMTP server.
User name:	User name used for authentication
Password:	Password used for authentication



4.9.5 Event Manager

4.9.5.1 Events

The system ships with a set of predefined system events. This menu can be used to set up notification messages in order to send a text message (SMS) or E-Mail to one or more recipients in case of such events.

Event	Event Text
PPP connection established	PPP connection up. ppp0 interface address: %PPP_IP%.
PPP connection down	PPP connection down.
PPP connection failure	PPP failure to connect. Error reported: %PPP_ERR%. See manual and logs to identify the problem.
WLAN connection established	WLAN connection up. interface address: %WLAN_IP%
WLAN connection down	WLAN connection down.
VPN connection established	VPN connection up. tun0/tap0 interface address: %VPN_IP%.
VPN connection down	VPN connection down.
VPN connection failure	VPN failure to connect. See logs to identify the problem.
Dial-in connection established	Dial-in connection establish: user: %DIN_USER% from: %DIN_IP%.
Dial-in connection down	Dial-in connection terminated: user: %DIN_USER% from: %DIN_IP%.
Dial-in connection failure	Dial-in failure to connect.
Dynamic DNS registration	DYNDNS update with %DYNDNS_IP% address.
Dynamic DNS failure to reach server	DynDNS failure to reach server.
Login to the Web Manager	Log-in to the Configuration GUI, by the user: %LOGIN_USER%.
Failed to Login to the Web Manager	Failed attempt to log-in to the Configuration GUI, by the user: %LOGIN_USER%.
Restart after power up	Restart after power up.
Restart due to a software exception	Restart due to a software exception.
Restart due to Web Manager	Restart due to Web Manager.
Startup completed	Startup completed
Arriving UDP Message	%UDP_MESSAGE%
Test Event	This is a test.
GPS reception on	GPS position is available.
GPS reception off	GPS position is not available.
Digital Input 1 on	Input change: IN1 is On.
Digital Input 1 off	Input change: IN1 is Off.
Digital Input 2 on	Input change: IN2 is On.
Digital Input 2 off	Input change: IN2 is Off.
Digital Output 1 on	Output change: OUT1 is On, changed from %DIO_SOURCE%.
Digital Output 1 off	Output change: OUT1 is Off, changed from %DIO_SOURCE%.
Digital Output 2 on	Output change: OUT2 is On, changed from %DIO_SOURCE%.
Digital Output 2 off	Output change: OUT2 is Off, changed from %DIO_SOURCE%.

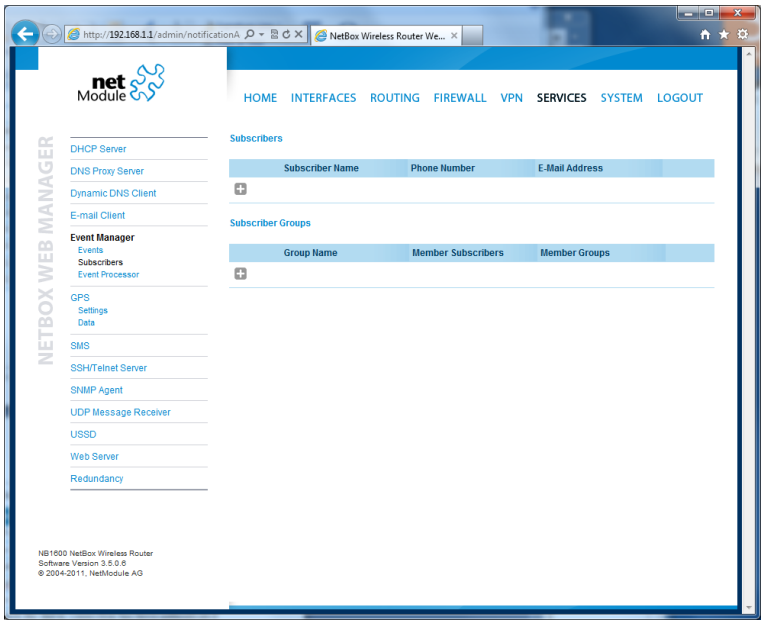
The following event variables will be replaced within event texts as follows:

Event Variables	Description
%PPP_IP%	The current IP address on the mobile interface (ppp0)
%PPP_ERR%	Error message in case of mobile connection failure
%VPN_IP%	The current address of the OpenVPN interface
%VPN_TYPE%	IPsec or OpenVPN
%DYNDNS_IP%	The IP address which has been sent to the DNS server
%DIN_USER%	User name which the dial-in connection has been authenticated against
%DIN_IP%	The IP address of the dial-in peer
%LOGIN_USER%	Name of the user who tried to log on to the Web Manager
%DIO_SOURCE%	Source that triggered an output change
%UDP_MESSAGE%	Text message that has been received by the message receiver
%RESTART_REASON%	Reason why a restart happened
%DST_IN1%	Status of digital input 1, possible values include [on, off]
%DST_IN2%	Status of digital input 2, possible values include [on, off]
%DST_OUT1%	Status of digital output 1, possible values include [on, off]
%DST_OUT2%	Status of digital output 2, possible values include [on, off]

4.9.5.2 Subscribers

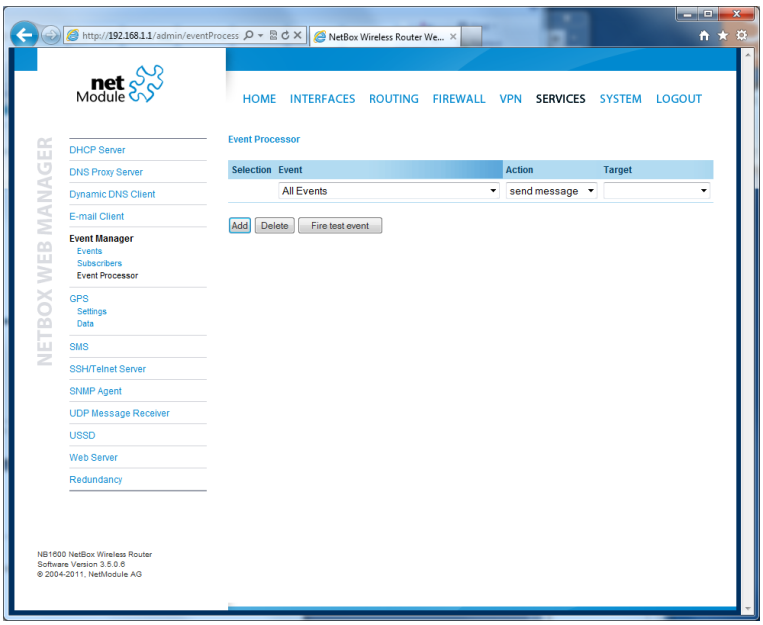
By setting up subscribers you can specify the recipients of SMS or E-Mail event notifications.

It is possible to create groups and populate them with users and other groups. By doing so, you can send event notifications to multiple destinations/users.



4.9.5.3 Event Processor

On this page you can configure how events shall be processed.



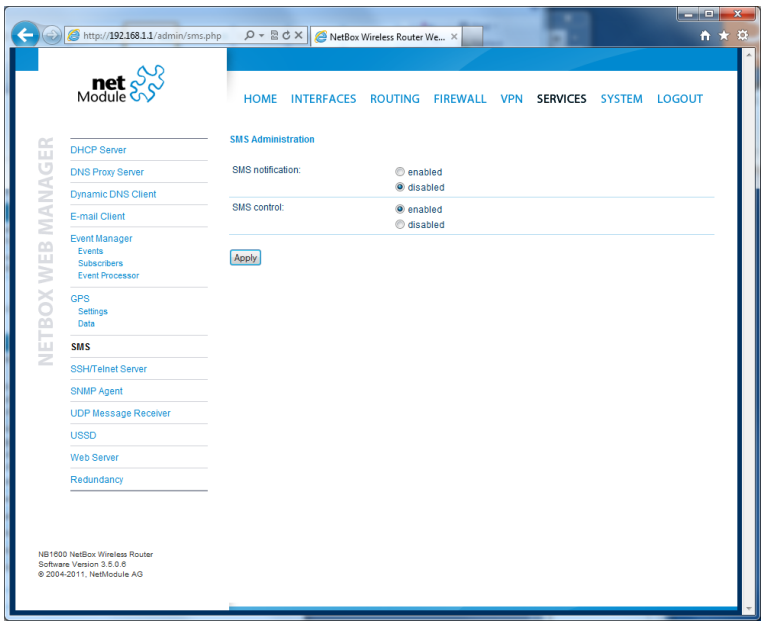
4.9.6 SMS

This page finally lets you turn on the SMS event notification service and enable remote control via SMS.

Parameter	Description
SMS notification:	Sending SMS can be enabled or disabled. Disabling sending SMS means that no notification via SMS will be performed.
SMS control:	Receiving SMS can be enabled or disabled. Disabling receiving SMS means that controlling NetBox via SMS will not be possible.

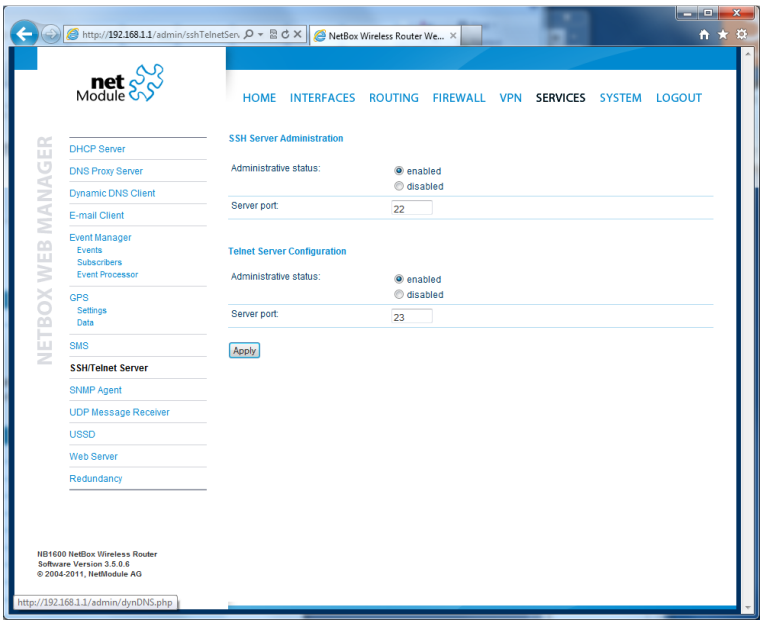
You may run the following commands on the box by simply sending a SMS to the phone number associated with the inserted SIM card:

Command	Parameters	Description
status	-	A SMS with the following information will be returned - Signal strength - Mobile connection state (up/down) - current IP address of the mobile interface - current IP address of the VPN interface (if enabled)
connect	-	This will initiate a Dial-out connection over GSM/UMTS and the VPN connection (if enabled) and trigger sending an SMS with the following information: - current IP address of the PPP interface - current IP address of the VPN interface (if enabled) The profile name is an optional parameter.
disconnect	-	terminates all WAN connections (including VPN))
reboot	-	Initiates a system reboot
method	manual	Set administrative status of the mobile connection to disabled
	permanent	Set administrative status of the mobile connection to enabled, permanent.
	dialonde-mand	Set administrative status of the mobile connection to enabled, dial on demand.
output	1 on	Switch digital output 1 on
	1 off	Switch digital output 1 off
	2 on	Switch digital output 1 on
	2 off	Switch digital output 2 off



4.9.7 SSH /Telnet Server

Parameter	Description
Administrative status:	Whether the SSH/Telnet service should be enabled/disabled
Port:	SSH/Telnet server port



4.9.8 SNMP Agent

The box is equipped with a SNMP daemon, supporting basic MIB tables (such as ifTable), plus additional enterprise MIBs to manage multiple systems.

The current range of system IDs:

NetBox Model	ID
NB1310	1.3.6.1.4.1.31496.10.10.50
NB1600	1.3.6.1.4.1.31496.10.10.46
NB2700	1.3.6.1.4.1.31496.10.10.47
NB3700	1.3.6.1.4.1.31496.10.10.48

Up to now the NetBox extensions contain support for:

- rebooting the device
- updating to a new system software via FTP/TFTP/HTTP
- updating to a new system configuration via FTP/TFTP/HTTP
- getting the status of last software update
- getting the status of last configuration update

Setting MIB values is limited to SNMPv3 and only the 'admin' user is entitled to trigger the extensions.

ATTENTION must be paid to the fact that SNMP passwords have to be more than 8 characters long. Shorter passwords will be doubled for SNMP, which for instance means 'admin01' becomes 'admin01admin01'.

The SNMP extensions can be read and triggered as follows:

- get system software version:

snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1 1.3.6.1.4.1.31496.10.40.1.0

- get kernel version:

snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1 1.3.6.1.4.1.31496.10.40.2.0

- get serial number:

snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1 1.3.6.1.4.1.31496.10.40.3.0

- restart the device:

snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1 1.3.6.1.4.1.31496.10.40.10.0 i 1

- run configuration update:

snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1 1.3.6.1.4.1.31496.10.40.11.0 s "http://server/directory"

REMARK: configUpdate expects a zip-file named <serial-number>.zip in the specified directory which contains at least a "user-config.zip"

Supported protocols are TFTP, HTTP(s= and FTP.

Specifying a username/password or port is not yet supported.

- get configuration update status:

snmpget -v 3 -u snmpadmin -n "" -l authNoPriv -a MD5 -x DES -A snmpadmin 192.168.1.1 1.3.6.1.4.1.31496.10.40.12.0

The return value can be one of: (1) succeeded, (2) failed, (3) inprogress, (4) notstarted.

- run software update:

snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1 1.3.6.1.4.1.31496.10.40.13.0 s "http://server/directory"

- get software update status:

snmpget -v 3 -u snmpadmin -n "" -l authNoPriv -a MD5 -x DES -A snmpadmin 192.168.1.1 1.3.6.1.4.1.31496.10.40.14.0

The return value can be one of: (1) succeeded, (2) failed, (3) inprogress, (4) notstarted.

Parameter	Description
SNMP agent status:	Enable or disable the SNMP agent.
Listening Port:	SNMP agent port
Community:	An SNMP community string corresponding to the group that devices and management stations running SNMP belong to.
Contact:	System maintainer/contact information

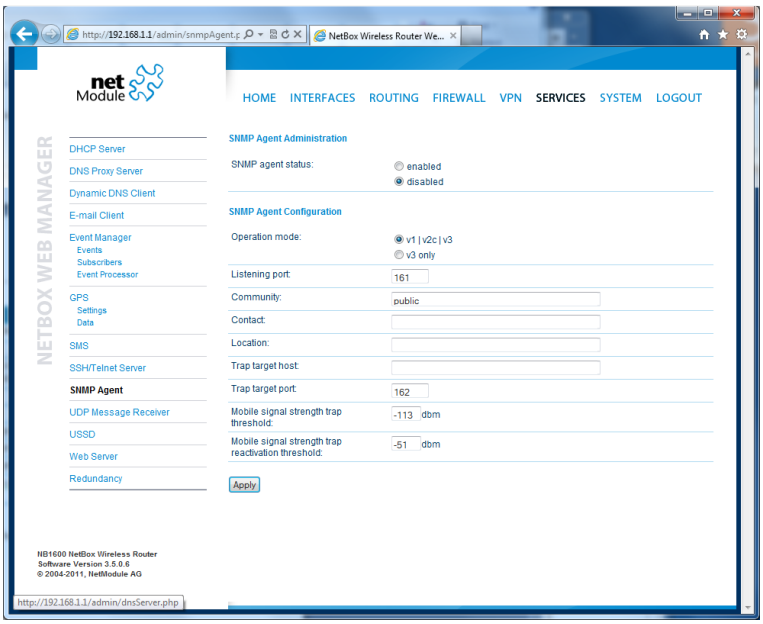
Location:	Location of the device
Trap target host:	The host where the traps will be sent to
Trap target port:	The port where the traps will be sent to
Signal strength trap threshold:	A trap will be sent, if signal strength falls below this threshold.
Signal strength trap reactivation threshold:	No further traps will be sent as long as signal strength his not higher than this value.

Once the SNMP agent is enabled, the SNMP traps are generated in case of the following conditions

- Start-up of the box
- Shutdown of the box
- VPN connected
- VPN disconnected
- Signal strength fell below „Signal strength trap threshold“

The start-up trap is implemented using the standard cold Start & warm Start traps.

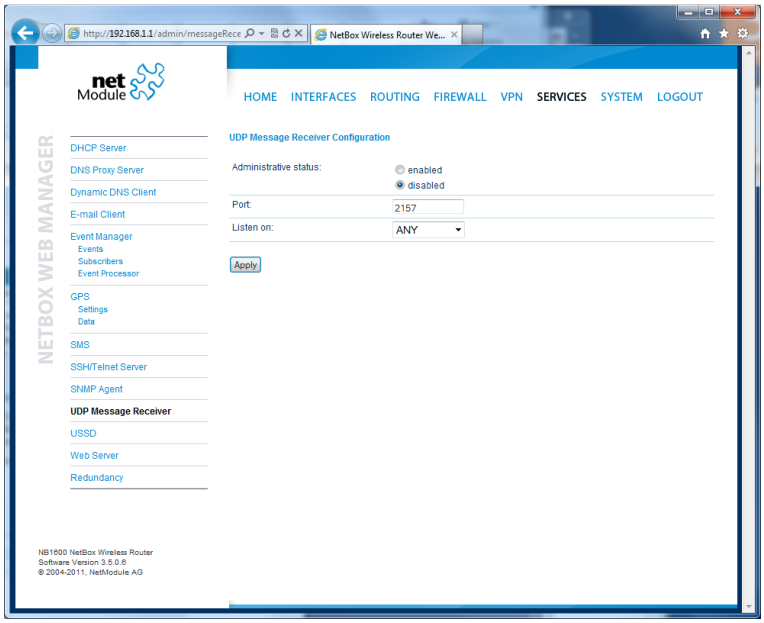
The system-shutdown trap is sent, when the system is rebooted via the reboot function of the web interface or when the watchdog reboots the system.



4.9.9 UDP Message Receiver

Parameter	Description
Port:	UDP message receiver port

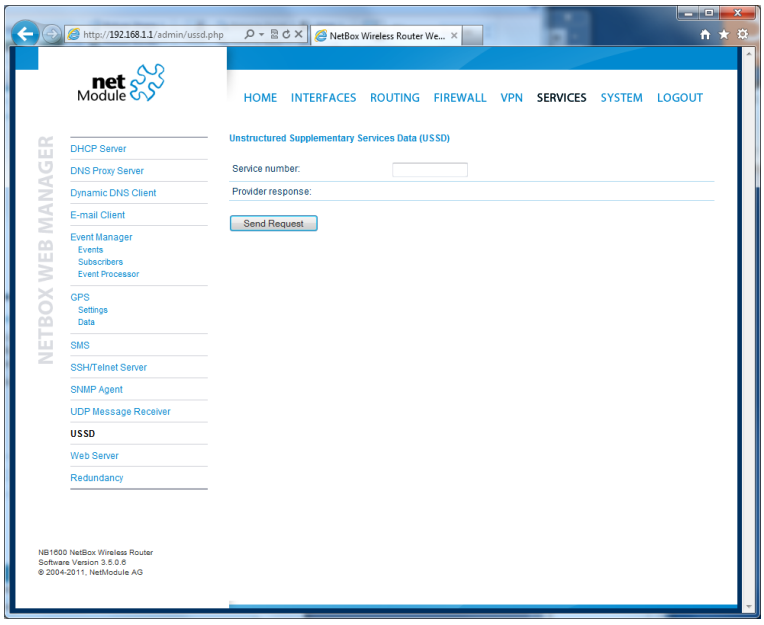
The UPD Message Receiver is a service that listens on the configured port (default 2157) for arriving UDP packets with a string in the payload. Once an UPD packet has arrived the event “Arriving UDP Message” is fired (see chapter 4.9.5.1 Events). Use the Event Manager (4.9.5 Event Manager) to forward the message (UDP payload) to a SMS or E-mail destination.



4.9.10 Unstructured Supplementary Services Data (USSD)

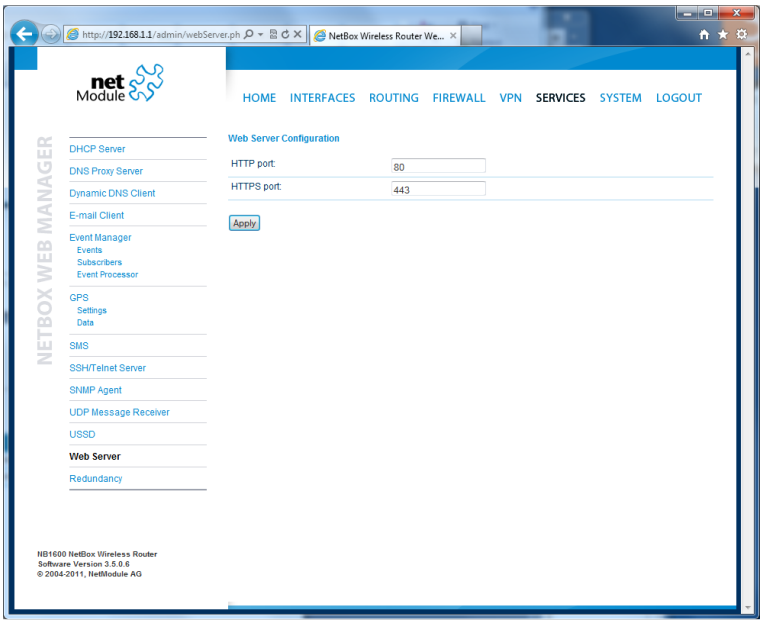
Unstructured Supplementary Services Data (USSD) is a GSM service that allows high speed interactive communication between the subscribers and applications across a GSM Network. A sample USSD service is the bill status service accessed by dialling *141# or similar numbers in between * and #.

Contact your mobile operator for further information.



4.9.11 Web Server

Parameter	Description
HTTP port:	Web server port for HTTP connections
HTTPS port:	Web server port for HTTPS connections



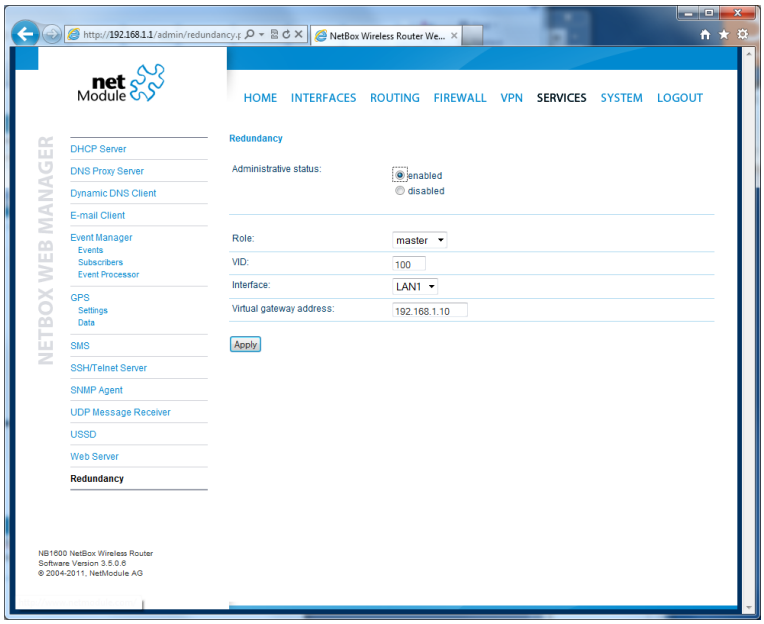
4.9.12 Redundancy

This section can be used to set up a redundant pair of boxes (or other systems) by running the Virtual Router Redundancy Protocol (VRRP) among them. A typical VRRP scenario defines a first host playing the master and another the backup device, they both define a virtual gateway IP address which will be distributed by gratuitous ARP messages for updating the ARP cache of all LAN hosts and thus redirecting the packets accordingly.

A takeover will happen within approximately 3 seconds as soon as the partner is not reachable anymore (checked via multicast packets). This may happen when one device is rebooting or the Ethernet link went down. Same applies when the WAN link goes down.

In case DHCP has been activated, please keep in mind that you will need to reconfigure the DHCP gateway address offered by the server and let them point to the virtual gateway address. In order to avoid conflicts you may turn off DHCP on the backup device or even better, split the DHCP lease range in order to prevent any lease duplication.

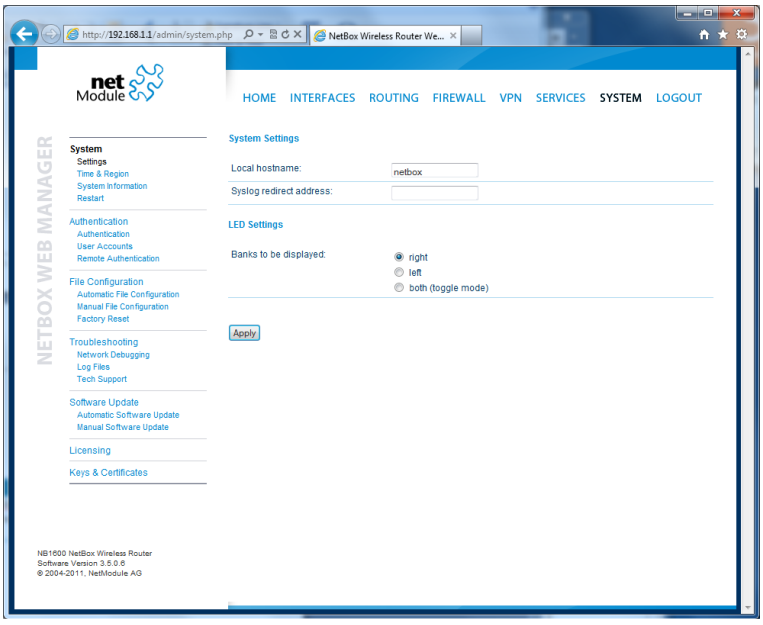
Parameter	Description
Administrative status:	Administrative status:
Role:	The role of this system (either master or backup)
VID:	The Virtual Router ID (you can theoretically run multiple instances)
Interface:	Interface on which VRRP should be performed
Virtual gateway address:	The virtual gateway address formed by the participating hosts.



4.10 System

4.10.1 Settings

Parameter	Description
Local host name:	The local host name of the system
Syslog redirect address:	The host where system log messages should be forwarded to. A tiny system log server for Windows is included in TFTP32 which can be downloaded from our website.
LED Settings:	You can configure the behaviour of the status LEDs on the front panel of your device. They are usually divided into two banks (left/right on NB1600, top/ bottom on NB2700) and are either indication the connection status or the digital IO port status. You may configure toggle mode, so that the LEDs periodically show both bank states.

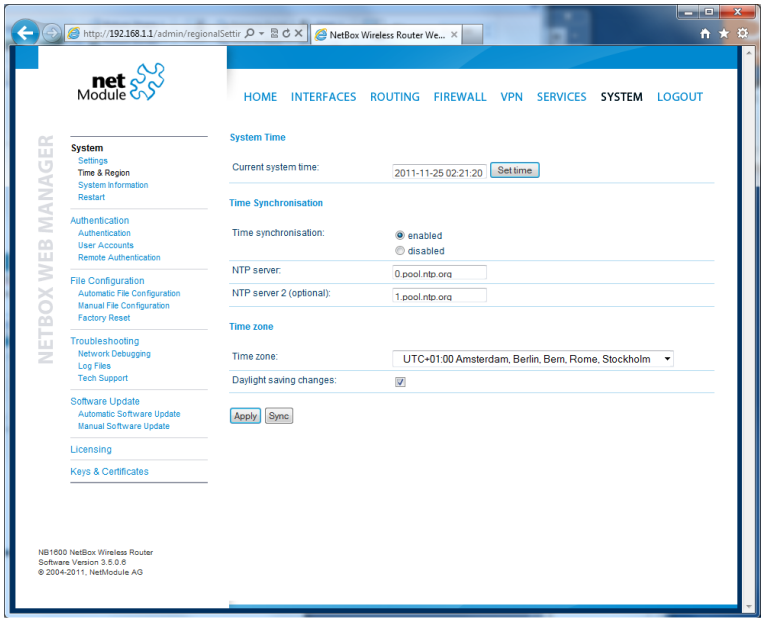


4.10.2 Time and Region

The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. NetBox can synchronize its system time with a NTP server or (if available) via GPS.

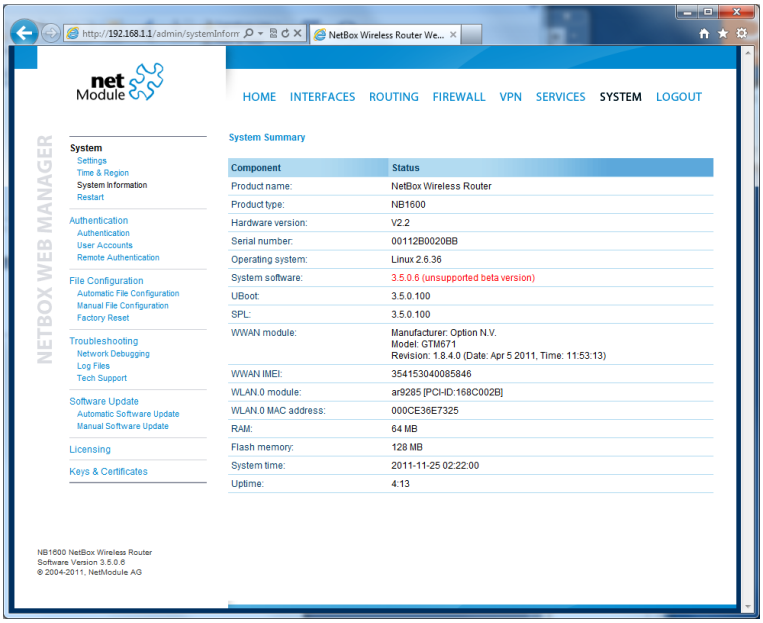
If enabled, the time synchronization is usually triggered after a WAN link has come up but before starting any VPN connections. Further time synchronizations are scheduled in background every 60 minutes.

Parameter	Description
NTP state:	Enable/disable time synchronization
NTP server:	Host name of NTP server
NTP server 2 (optional):	Host name of an optional second NTP server
Time zone:	Time zone
Daylight saving changes:	This option can be used to reflect daylight saving changes (e.g. switching from summer to winter time) depending on the selected time zone.



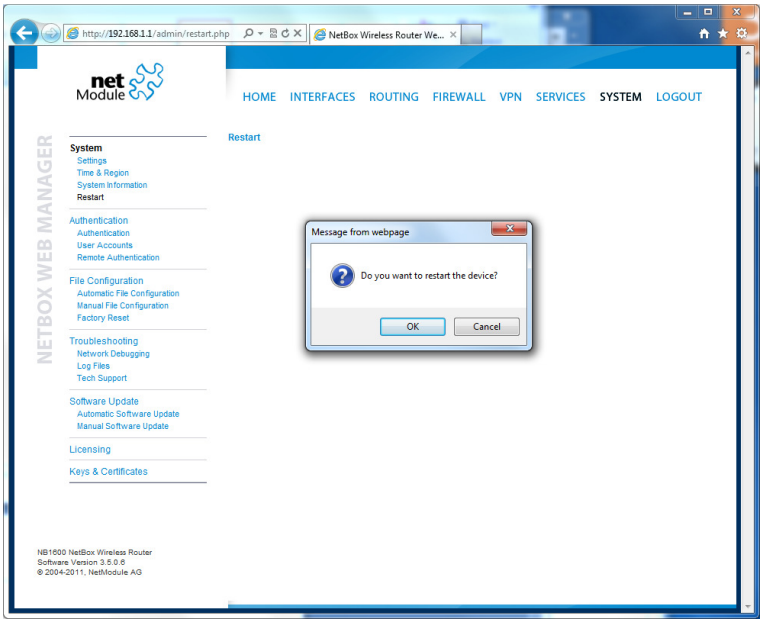
4.10.3 System Information

The system information page displays various details of your box:

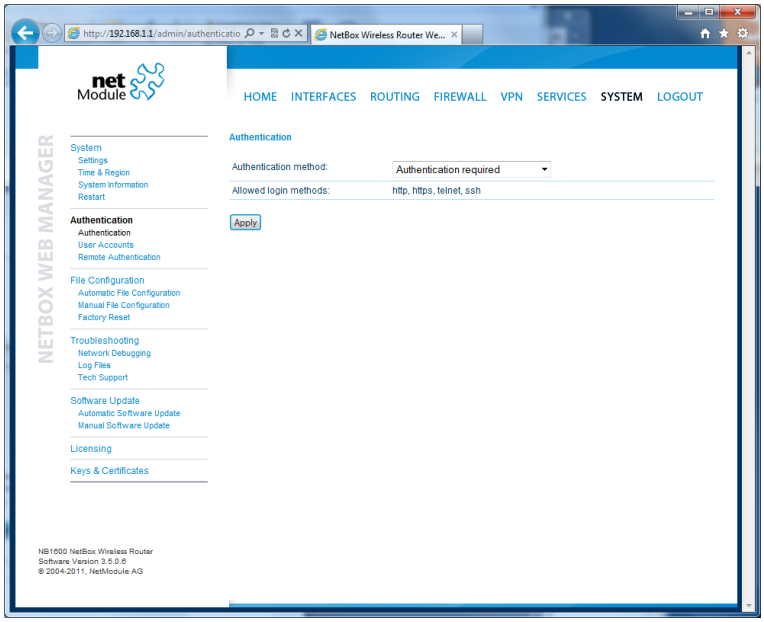


4.10.4 Restart

This menu can be used to restart the system. Any WAN links will be dropped.



4.10.5 Authentication

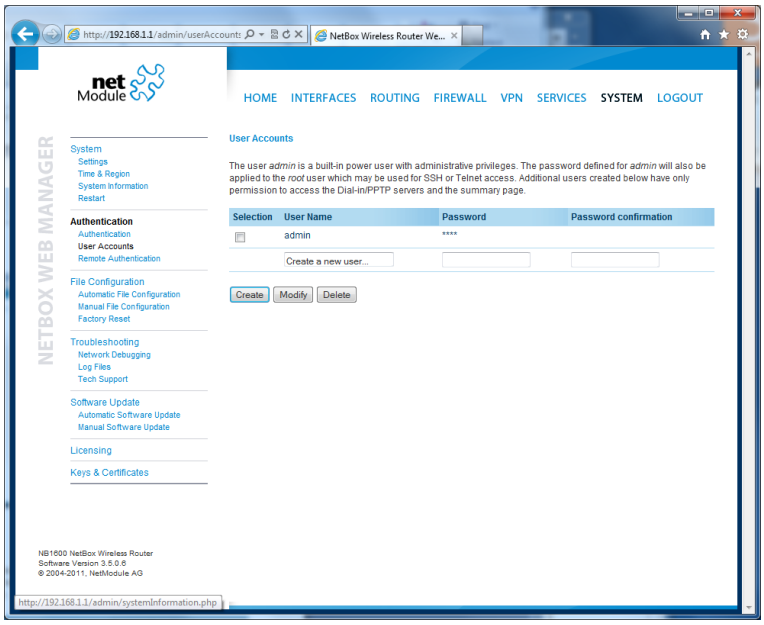


4.10.6 User Accounts

This page lets you manage the user accounts on the device.

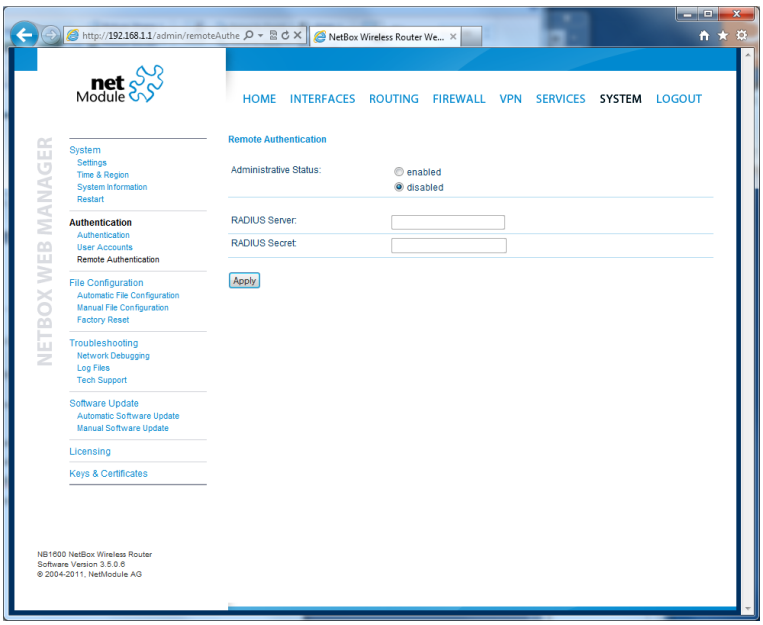
The standard **admin** user is a built-in power-user that has permission to access the Web Manager the Dial-in server and other administrative services. Any other user only has permission to view the status page or can be used for dial-in connections.

Parameter	Description
User name	Define a user name
Enter password:	Define a password
Re-enter password:	Confirm the password



4.10.7 Remote Authentication

A remote RADIUS server can be used to authenticate users. This applies for the Web Manager, the WLAN network and other services supporting RADIUS.



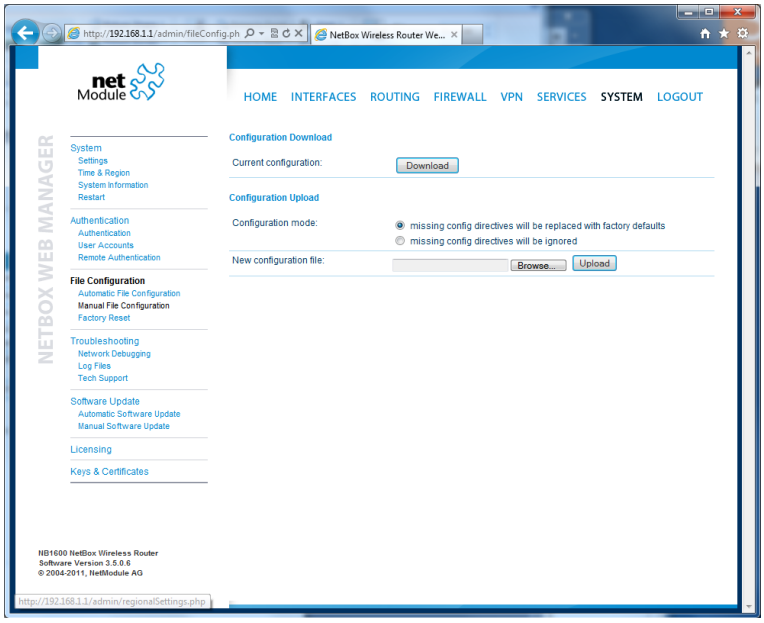
Parameter	Description
Administrative status	Defines whether remote authentication should be used or not
RADIUS server	The RADIUS server address
RADIUS secret	The secret used to authenticate against the RADIUS server
Authentication port	The port used for authentication
Accounting port	The port used for accounting messages
Use for login	This option enables remotely-defined users to access the Web Manager

4.10.8 File Configuration

Configuration via the Web Manager becomes tedious for large volumes of devices. NetBox therefore offers automatic and manual file-based configuration to automate things. Once you have successfully set up the system you can back up the configuration and restore the system with it afterwards. You can either upload a single configuration file (.cfg) or a complete package (.zip) containing the configuration file and a packed version of other essential files (such as certificates).

4.10.8.1 Automatic File Configuration

Parameter	Description
Status:	Enable/disable automatic configuration update
Time of day:	Time of day when the system will check for updates
URL:	The server URL where the configuration file should be retrieved from (supported protocols are HTTP(s), TFTP, FTP).
Last config update:	The result of the last configuration update attempt



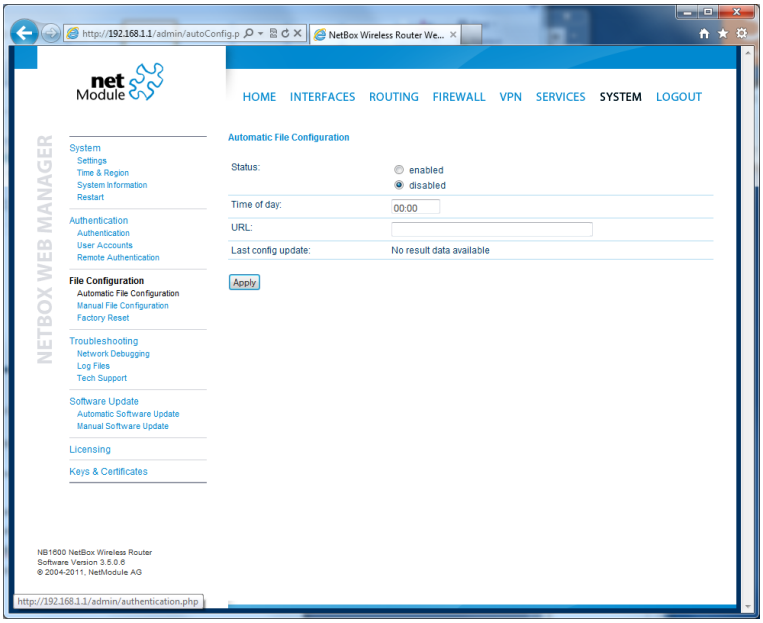
4.10.8.2 Manual File Configuration

This section can be used to download the currently running system configuration (including essential files such as certificates).

Parameter	Description

In order to restore a particular configuration you can upload a configuration previously downloaded.

You can choose between missing configuration directives set to factory defaults or getting ignored, that means, potentially existing configuration directives will be kept at the system.



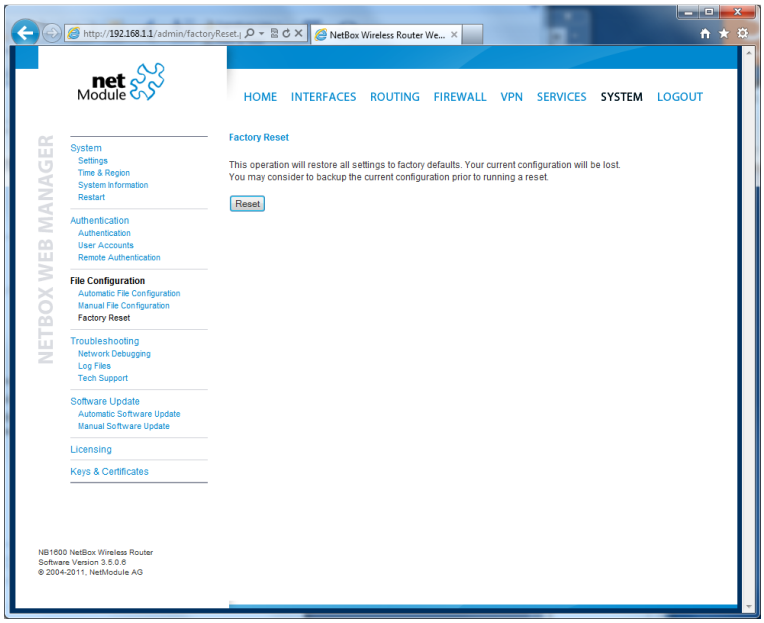
4.10.8.3 Factory reset

This menu can be used to reset the device to factory defaults. Your current configuration will be lost.

This procedure can also be initiated by pressing and holding the Reset button for at least five seconds. A successfully initiated factory reset can be noticed by all LEDs having been turned on.

The factory reset will set the IP address of the first Ethernet interface back to 192.168.1.1. You will be able to communicate again with the device using the default network parameters.

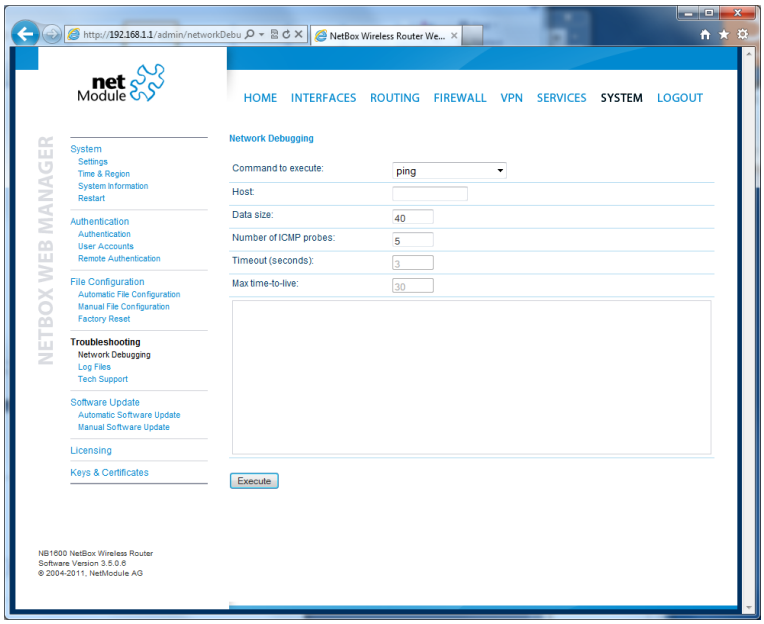
You may store the currently running configuration as factory defaults which will reside active even when a factory reset has been initiated (e.g. by your service staff). Please ensure that this corresponds to a working configuration. A real factory reset to the default settings can be achieved by restoring the original factory configuration and initiating the factory reset again.



4.10.9 Troubleshooting

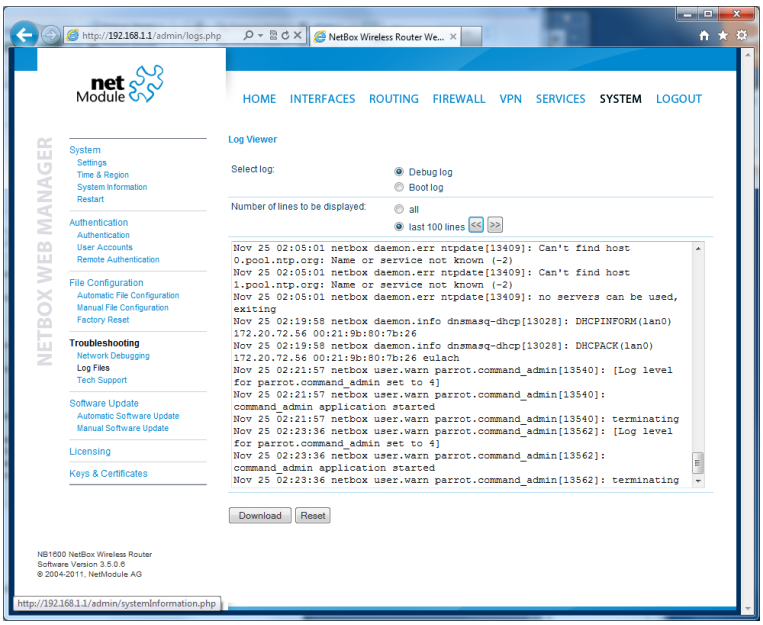
4.10.9.1 Network Debugging

Various tools reside on this page for further analysis of potential configuration issues.



4.10.9.2 Log Files

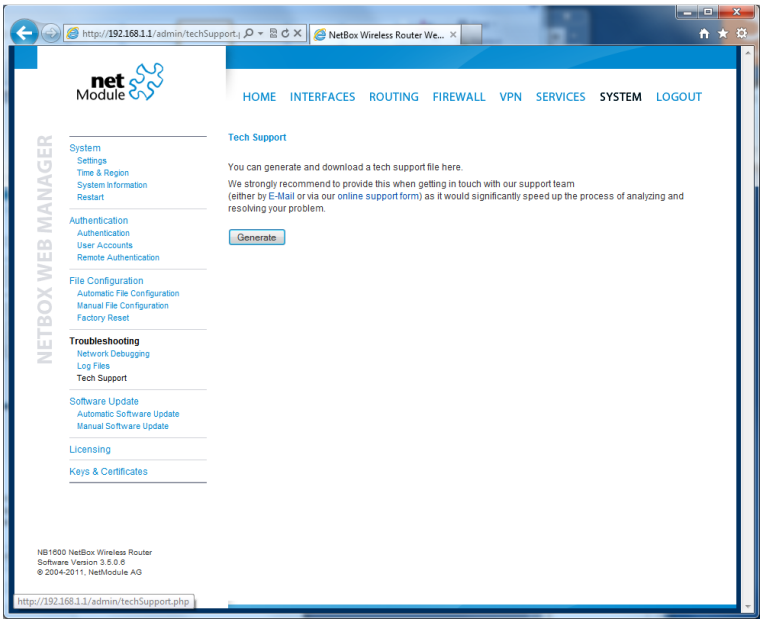
Log files can be viewed a downloaded and reset here. Please study them carefully in case of any issues.



4.10.9.3 Tech Support

You can generate and download a tech support file here.

We strongly recommend providing this file when getting in touch with our support team, either by e-mail or via our online support form, as it would significantly speed up the process of analyzing and resolving your problem.


HOME INTERFACES ROUTING FIREWALL VPN SERVICES SYSTEM LOGOUT
Tech Support
You can generate and download a tech support file here.
We strongly recommend to provide this when getting in touch with our support team
(either by E-Mail or via our online support form) as it would significantly speed up the process of analyzing and
resolving your problem.
Generate

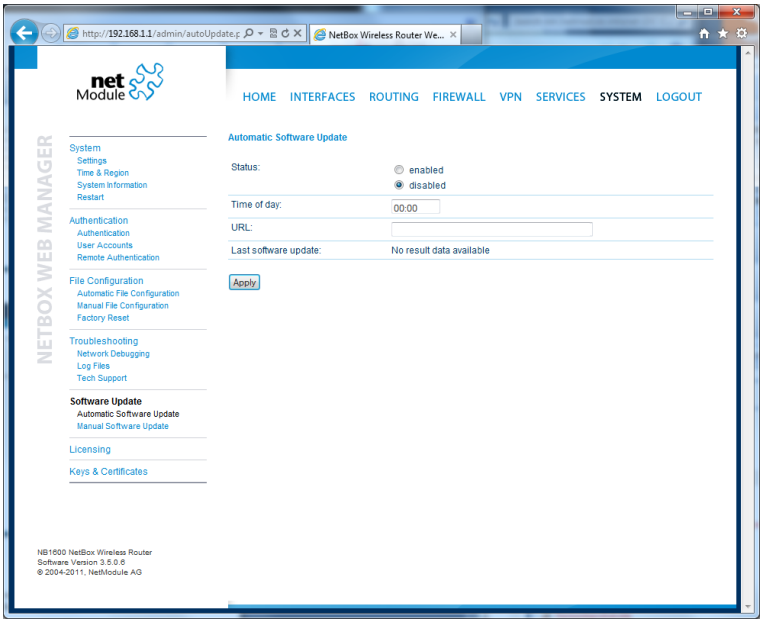
4.10.10 Software Update

Software upgrade from the last official software release to the current release published on www.netmodule.com is supported. For further details please consult the release note.

Software downgrade is not supported. Software downgrade may lead to loss of configuration and inaccessibility of the device.

4.10.10.1 Automatic Software Update

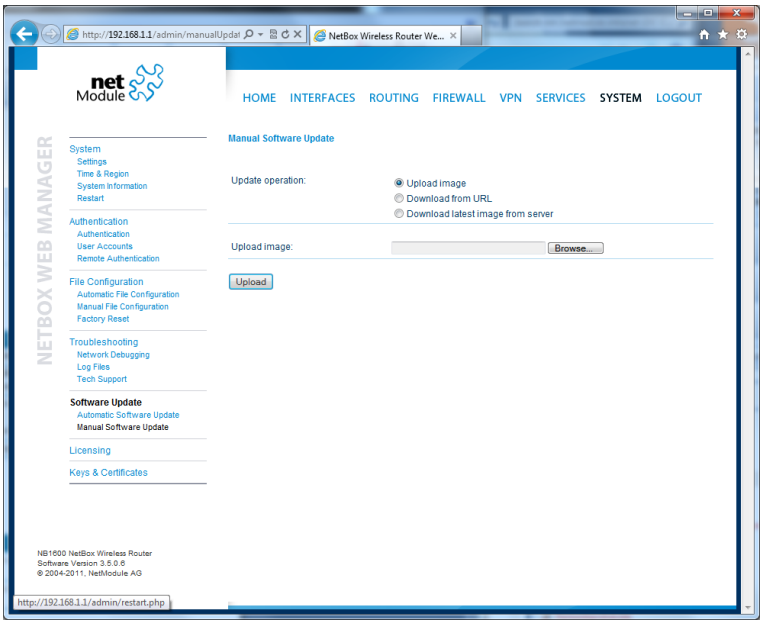
Parameter	Description
Status:	Enable/disable automatic software update
Time of day:	Every day at this time NetBox will do a check for updates
URL:	The server URL where the software update package should be downloaded from. Supported protocols are TFTP, HTTP(s), and FTP.
Last software update:	The result of the last software update attempt.



4.10.10.2 Manual Software Update

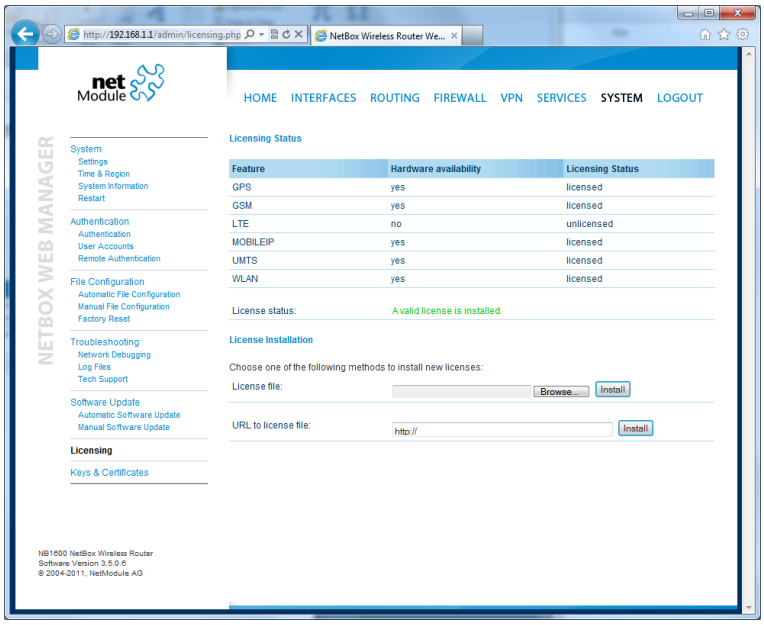
This menu can be used to run a manual software update of the system:

Parameter	Description
Update operation	The update operation method being used. You can upload the image, download it from an URL or use the latest version from our server.
URL	The server URL where the software update image should be downloaded from. Supported protocols are TFTP, HTTP(s), and FTP.



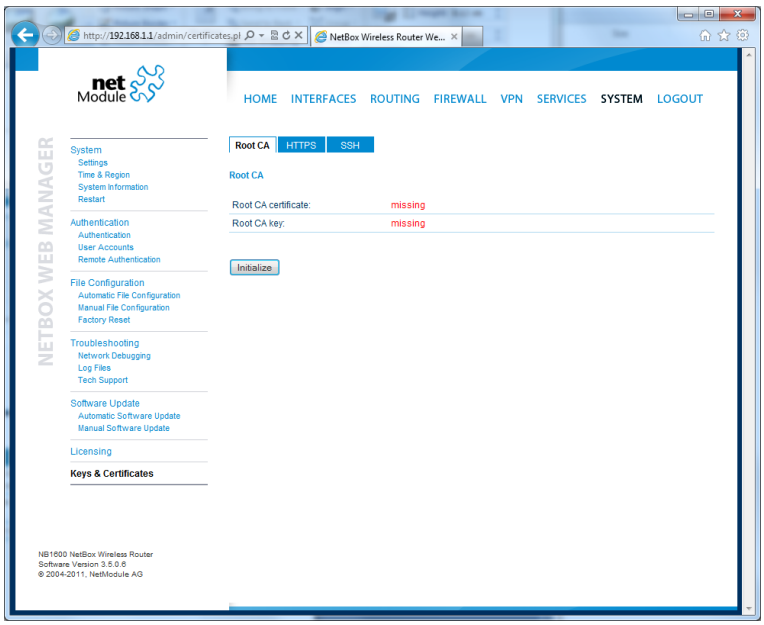
4.10.11 Licensing

This menu allows you to view and update the license status of your system. Note that some features are disabled if no valid license is provided.



4.10.12 Keys and Certificates

The key and certificate page lets you generate required files for securing your services (such as the HTTP and SSH server). Keep in mind that you will need to create keys and certificates for OpenVPN in case of certificate based authentication. You can also revoke and invalidate certificates again (for instance if they have been compromised or lost).



4.11 Logout

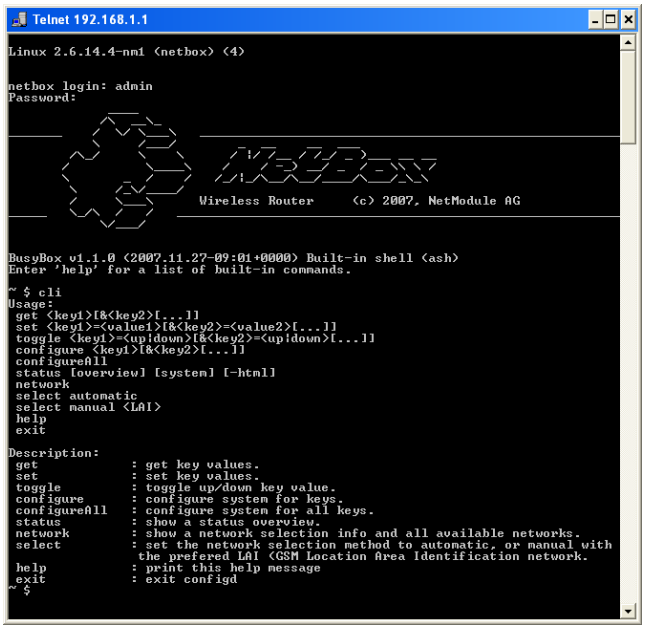
Log out from Web Manager

5 Configuration via Command Line Interface (Advanced)

The command line interface is accessible after successful login to NetBox via telnet or Secure Shell (SSH). By default the telnet server answers on port 23, the SSH server on port 22.

192.168.1.1 - PuTTY
login as: admin
admin@192.168.1.1's password:
Wireless Router (c) 2007, NetModule AG
BusyBox v1.1.0 (2007.11.27-09:01+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

Logon via SSH with PuTTY


Telnet 192.168.1.1
Linux 2.6.14.4-nm1 (netbox) (4)
netbox login: admin
Password:
Wireless Router (c) 2007, NetModule AG
BusyBox v1.1.0 (2007.11.27-09:01+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.
~ $ cli
Usage:
get <key1>[&<key2>[...]]
set <key1>=<value1>[&<key2>=<value2>[...]]
toggle <key1>=<up|down>[&<key2>=<up|down>[...]]
configure <key1>[&<key2>[...]]
configureAll
status [overview] [system] [-html]
network
select automatic
select manual <LAI>
help
exit
Description:
get : get key values.
set : set key values.
toggle : toggle up/down key value.
configure : configure system for keys.
configureAll : configure system for all keys.
status : show a status overview.
network : show a network selection info and all available networks.
select : set the network selection method to automatic, or manual with the prefered LAI (GSM Location Area Identification network.
help : print this help message
exit : exit configd
~ $

Logon via Telnet via Windows Telnet Client

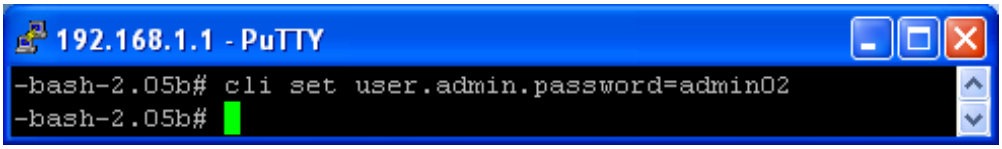
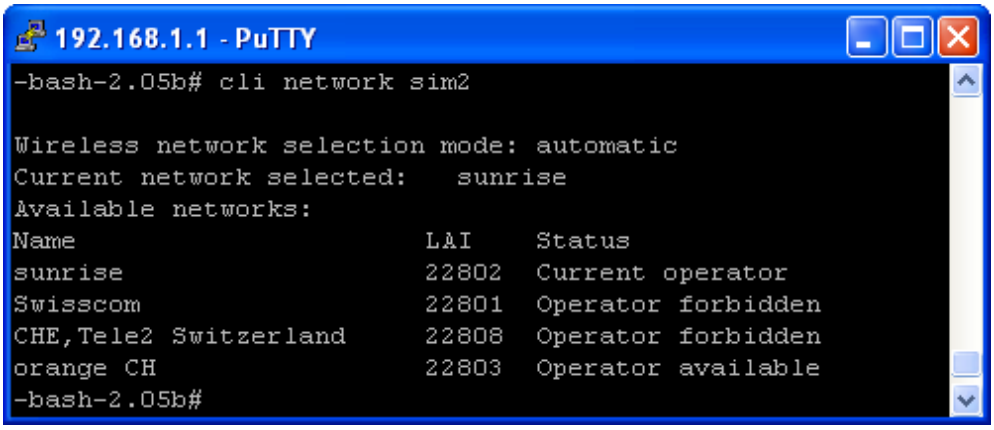
After authentication, type “cli help” into the Shell to learn about the usage of the command line interface. CLI will stop after every call. You have to include ‘cli’ for every new call.

5.1 CLI Overview

The Command Line Interface mainly provides functions to read and write values of the NetBox configuration parameters. In addition, the CLI provides functions to query status information.

Command	Return	Description
cli get	string	Read values of one or more specified configuration parameters.
cli set	void	Write values of one or more specified configuration parameters.
cli network	string	Show available networks including Location Area Identities (LAIs)
cli select	void	Select the network provider defined by the supplied Local Area Identity (LAI) or set the network selection method to automatic
cli status	string	Show a status overview of NetBox
cli help	string	Print the cli help message (usage)
Ctrl+C	void	Abort a command. Exit from CLI

5.2 CLI Usage

Command	Usage and Return Value
cli get	'cli get' is used to read values from configuration parameters. Arguments include all configuration keys as described in chapter 3.2 Usage: cli get <key1>[&<key2>[...]] Example: cli get user.admin.password The return value is the value of the queried parameter. Note: cli get <invalidKey> returns no error message
cli set	'cli set' is used to assign values to configuration parameters. Arguments include all configuration keys as described in chapter 3.2 Usage: set <key1>=<value1>[&<key2>=<value2>[...]] Example: cli set user.admin.password=admin02  'cli set' produces no return value and no error message. To check if the modification took place, use 'cli get' Note: cli set <invalidKey>=<correctValue> returns no error message Note: cli set <validKey>=< inCorrectValue> returns no error message, no range check is performed
cli network	'cli network' provides mobile network information on the optionally specified SIM card. If no SIM card is specified, the command is applied to SIM1. The information returned includes the Local Area Identity (LAI) Usage: network [sim1/sim2] Example: cli network sim2  Note: The following commands are identical: 'cli network' and 'cli network sim1'
cli select automatic	'cli select automatic' sets the network selection mode for the specified SIM card to automatic. Usage: select automatic [sim1/sim2]

Command	Usage and Return Value
	Note: The following commands are identical: 'cli select automatic' and 'cli select automatic sim1' Note: The following commands have the same effect: 'cli select automatic sim1' and 'cli set networkselection.mode=automatic' 'cli select automatic sim2' and 'cli set networkselection.sim2.mode=automatic'
cli select manual	'cli select manual' selects the network provider defined by the supplied Local Area Identity (LAI) for the specified SIM card Usage: select manual <LAI> [sim1/sim2] Note: The following commands are identical: 'cli select manual <lai>' and 'cli select manual sim1 <lai>' Note: The following commands have the same effect: 'cli select manual <lai> sim1' and 'cli set networkselection.network_lai=<lai>' 'cli select manual <lai> sim2' and 'cli set networkselection.sim2.network_lai=<lai>'

Command	Usage and Return Value
cli status	'cli status' returns both, 'cli status overview' and 'cli status system' concatenated. The option -hml is used to query a HTML version of the status information.
cli status overview	show the status of all interfaces, networks and services.
cli status overview interfaces	show the status of all interfaces
cli status overview interfaces sim_state	show the state of the SIM-Card
cli status overview interfaces pin_state	show the state of the PIN
cli status overview interfaces signal_strength	show the actual signal strength
cli status overview interfaces con_state	show the state of the wireless connection
cli status overview interfaces con_type	show the type of the wireless connection
cli status overview interfaces net_sel_mode	show the mode of the network selection
cli status overview interfaces net_sel_prov	show the current network provider
cli status overview interfaces data_rxtx	show the amount of received and transmitted data
cli status overview interfaces stream_updown	show the actual down- and upstream rates
cli status overview interfaces last_reset	show the last reset date of data counter
cli status overview networks	show the status of all networks
cli status overview networks napt_state_mob	show the state of the NAPT service on the mobile if
cli status overview networks napt_state_ovpn	show the state of the NAPT service on the vpn if
cli status overview networks openvpn_state	show the state of the OpenVPN connection
cli status overview networks ipsec_state	show the state of the IPsec connection
cli status overview networks pptp_state	show the state of the PPTP server
cli status overview services	show the status of all services
cli status overview services dyndns_state	show the state of the Dynamic DNS client
cli status overview services dialin_state	show the state of the Dial-in service
cli status overview services dhcp_state	show the state of the DHCP server
cli status overview services dns_state	show the state of the DNS Proxy server
cli status overview services gps_state	show the state of the GPS signal
cli status overview services keepalive_state	show the state of the Keep-alive service
cli status overview services sms_rec_state	show the state of the SMS receiving service
cli status overview services sms_send_state	show the state of the SMS sending service
cli status overview services email_state	show the state of the E-Mail service
cli status overview services dig_in	show the state of the digital inputs
cli status overview services dig_out	show the state of the digital outputs
cli status system	show NetBox systems information including hardware and software versions.
cli status system prod_name	show the NetBox product name
cli status system prod_type	show the NetBox product type
cli status system hw_ver	show the NetBox hardware version
cli status system serial	show the NetBox serial number

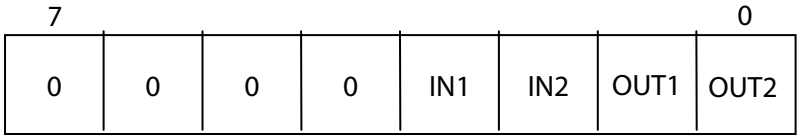
Command	Usage and Return Value
cli status system os	show the NetBox operating system
cli status system nbsw	show the NetBox software version
cli status system cpu	show the NetBox CPU
cli status system wireless_module	show the NetBox wireless module
cli status system ram	show the amount of RAM installed in the NetBox
cli status system flash	show the amount of flash installed in the NetBox
help	Print the cli help message (usage)

6 Software Interfaces

6.1 Digital I/O Server

In order to manage digital inputs and outputs via TCP an additional piece of software is required on the host that handles the TCP connection and sets the ports respectively. For test purposes telnet can be used. The payload must contain the states of the four inputs/outputs ports as follows:

The value 0 represents the state “off”, the value 1 the state “on”.



6.1.1 Monitor the digital inputs and outputs

Every digital input change triggers a message of the described format. It also contains the valid states of the outputs.

6.1.2 Set digital outputs

In order to set the digital I/O port states you may send the following pattern (ASCII characters)

Pattern	Description
00000000	Turn all digital outputs off
00000001	Turn output 2 on, turn output 1 off
00000010	Turn output 1 on, turn output 2 off
00000011	Turn output 1 on, turn output 2 on

6.1.3 Get status of digital inputs and output

To get the states of the digital I/O ports you may send the following pattern (ASCII characters)

Pattern	Description
00010000	Request a message with all states

6.2 HTTP Service Interface

The HTTP service interface is designed to administrate the NetBox with a common http client.

It basically consists of a set of web pages (PHP) located in the root directory of the web server:

- login.php (used by HTTP clients to log in)
- logout.php (used by HTTP clients to log out)
- upload.php (can be used to upload configuration files)
- download.php (can be used to download log files)
- cli.php (the HTTP version of the CLI, offers the same command set)

Further documentation and help for utilizing the HTTP service can be provided on demand.

6.2.1 Command Set

General Restrictions:

- When sending parameters within HTTP GET requests, dots (.) within variables must be replaced by colons (:). Example: The key name **user.admin.password** results in **user:admin:password**
- Authentication is required for all commands except GET /cli.php?status,[parameters]

HTTP Request	Description
GET /cli.php?status,[parameters]	Takes the same parameters as the CLI
GET /cli.php?get,[parameters]	Takes the same parameters as the CLI
GET /cli.php?set,[parameters]	Takes the same parameters as the CLI
GET cli.php?sw-update,url=<URL>	Starts a software update by downloading the new software from a server. Supportes protocols include http, https, ftp, tftp, file Credentials can be specified as follows: ftp://user:pass@hostname:port/path
GET /cli.php?sw-update,path=<value>	Starts a local software update from a TFTP server (only use it for backward compatibility)
GET /cli.php?reboot	Restarts the NetBox
GET /login.php?usr=<user>,pwd=<password>	Login to the HTTP Service Interface with supplied credentials
GET /logout.php	Logout from the HTTP Service Interface
GET /download.php?file=<fileName>	Download a file • Debug log: file=debuglog • Boot log: file=bootlog
POST /upload.php	Takes a new configuration file as user-config.cfg or as user-config.zip. The content of the file must be the same as provided for the Web Manager.

6.2.2 Responses

HTTP Request	Responses (String)	Description
All HTTP Service Interface Commands	0: device busy	The NetBox is busy, please try again later
All HTTP Service Interface Commands	0: login required	This command requires authentication. Please use login.php first
GET /cli.php?status,[parameters]	<status>	A single or multiline string with the requested status information
GET /cli.php?get,[parameters]	<parameterValue>	The value of the requested configuration parameter
GET /cli.php?set,[parameters]	0: set failed	HTTP transfer is ok, but changing the configuration parameter failed.
	1: set ok	
GET /cli.php?sw-update,path=<value>	1: sw-update started from <path>	Software update started. Afterwards request the Software version with cli.php?status to verifiy whether it was successful or nor not
	0: maximum length of path is 26 characters	
	0: syntax error	Wrong syntax after in sw-update parameters
GET /cli.php?reboot	1: reboot initiated	A restart has been initiated
GET /login.php?usr=<user>,pwd=<password>	1: already logged in	
	1: already logged in but supplied credentials do not match	Already logged in but supplied credentials do not match
	1: login ok	Logged in successfully
	0: login failed	Login failed
GET /logout.php	1: logout ok	Logout OK
	1: already logged out	You were not logged in
GET /download.php?file=<fileName>	0: download <fileName> failed	Download failed
POST /upload.php	1: upload ok, files replaced, reconfiguration started	Upload ok, the provided files (e.g. OpenVPN certificates) were updated, the user-config.cfg will be applied
	1: upload ok, files replaced	No user-config.cfg provided but other files were updated (e.g. OpenVPN certificates)
	0: upload failed: <errorMessage>	The upload failed

6.2.3 Examples

HTTP Request	Command	Description
Query the NetBox Firmware Version via HTTP	`GET /cli.php?status,system,nbsw HTTP/1.1`	
Login	`GET /login.php?usr=admin,pwd=<password> HTTP/1.1`	
Set the admin Password	`GET /cli.php?set,user:admin:password=<password> HTTP/1.1`	Remember: The dots (.) must be replaced by colons (:)

Upload new Configuration Files	`POST /upload.php HTTP/1.1`
	`Content-Disposition: form-data; name="UserConfigFile"; filename="user-config.zip"`
	`Content-Type: application/x-zip-compressed`
	`[Media]`
		A zip archive containing the user configuration and other essential system files (such as keys or expert configurations)

Download Debug Log	`GET /download.php?file=debuglog HTTP/1.1`	
Restart the NetBox	`GET /cli.php?reboot HTTP/1.1`	
Logout	`GET /logout.php HTTP/1.1`	
Start a local software update	`GET /cli.php?swupdate,path=<server/path> HTTP/1.1`	

7 Troubleshooting

7.1 Error Messages

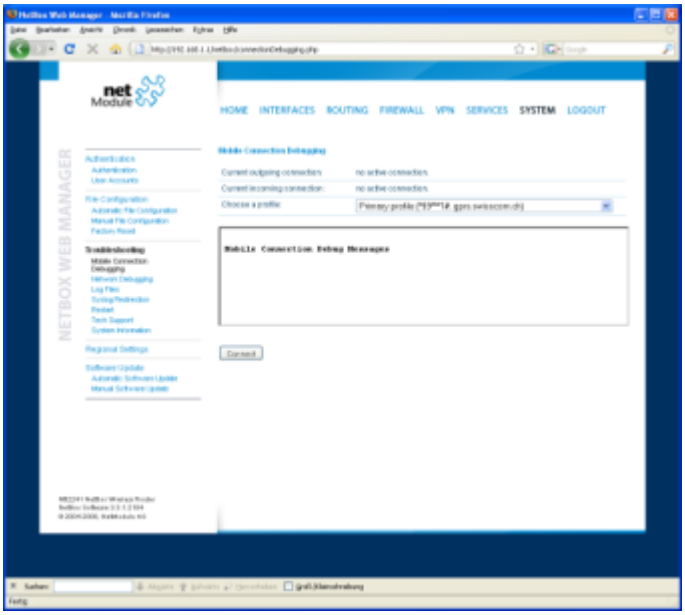
In general, the Web Manager will throw error messages upon failures in the status bar located in the footer of the corresponding web page.

Common error messages are:

Error Message	Problem Solving
SIM missing	Insert a SIM card
PIN code required	Insert the PIN code on the “SIM” page
Connection failed	See the “Debug Log” under Check APN, phone number, username, password

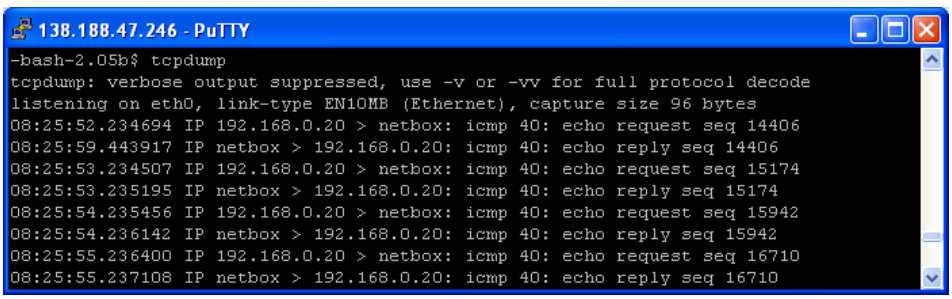
7.2 System Log and Log Files

Find more information about troubleshooting tools on page 64. The Web Manager also provides various debugging tools under SYSTEM/Troubleshooting:



7.3 Network Protocol Analyzer

It is possible to trace any IP interface and inspect individual packet flows between hosts. This can be achieved by logging onto the box and start a network packet capture by using the tool **tcpdump**. It is suggested to use the **–n** switch to bypass name resolution (e.g. **tcpdump –n –i lan0**). You may also generate a dump in PCAP format with **tcpdump –n –i lan0 –s 1500 –w /tmp/dump**, copy the file (e.g. via scp) and perform further inspection with **wireshark** (which is available at http://www.wireshark.org).


138.188.47.246 - PuTTY
-bash-2.05b$ tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
08:25:52.234694 IP 192.168.0.20 > netbox: icmp 40: echo request seq 14406
08:25:59.443917 IP netbox > 192.168.0.20: icmp 40: echo reply seq 14406
08:25:53.234507 IP 192.168.0.20 > netbox: icmp 40: echo request seq 15174
08:25:53.235195 IP netbox > 192.168.0.20: icmp 40: echo reply seq 15174
08:25:54.235456 IP 192.168.0.20 > netbox: icmp 40: echo request seq 15942
08:25:54.236142 IP netbox > 192.168.0.20: icmp 40: echo reply seq 15942
08:25:55.236400 IP 192.168.0.20 > netbox: icmp 40: echo request seq 16710
08:25:55.237108 IP netbox > 192.168.0.20: icmp 40: echo reply seq 16710

8 Customer Service

8.1 Technical Support

Further technical support can be accessed via the NetModule Website at:

http://www.netmodule.com/support

You will also find a download area where you can download the latest software and documentation material.

For support requests please use the support form available at:

http://www.netmodule.com/support/supportform.aspx

8.2 Feedback

Your feedback is highly appreciated; please send comments, suggestions, feature requests, error reports or your personal user experience with NetBox wireless routers to:

netbox@support.netmodule.com

Remember to have fun,

The NetBox team and its supporters

9 Notes